LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Security and Privacy in the Smart City

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Sofia Gustafsson
Amilia Åkesson

Supervisor: Miranda Kajtazi

Examiners: Odd Steen
Bo Andersson

Security and Privacy in the Smart City

AUTHORS: Sofia Gustafsson and Amilia Åkesson

PUBLISHER: Department of Informatics, Lund School of Economics and Management,
Lund University

PRESENTED: June, 2019

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Odd Steen, Associate Professor, PhD

NUMBER OF PAGES: 172

KEY WORDS: Smart City, security, privacy, challenges, solutions

ABSTRACT (MAX. 200 WORDS):

The number of Smart Cities have evolved in recent years and the concept is expanding in cities worldwide. Smart Cities have many potential advantages but to achieve these advantages Smart Cities must protect security and individual privacy. Addressing existing challenges in certain areas becomes critical to achieve further improvement and security and privacy concerns are very important in the Smart City because of the increasing number of Smart Cities around the world. Therefore, the aim of this study is to investigate in what ways Smart Cities work with security and privacy challenges. The study is based on a research model that is developed from a literature review on security and privacy challenges, consequences of challenges and solutions to challenges. Our results show that Smart Cities work with technology-, policy, regulatory and legal-, and governance and management solutions and they are all together very important. The results indicate that the Smart Cities work with leadership and planning when it comes to security and privacy. However, objectives for security and privacy, and also education and training related to security and privacy in the Smart Cities are things they do not work with today which needs more consideration.

Content

Figures

Tables

1 Introduction

1.1 Background

The concept of Smart Cities has in the past two decades received increased attention in both the industrial and academic field due to its strong realistic requirement and practical background in an increasingly urbanized world (Cui, Xie, Qu, Gao, & Yang, 2018). Smart Cities have evolved in recent years and the concept is expanding in the cities around the world (Edwards, 2017). A Smart City is a city that integrates modern technologies for automated and efficient service providing to enhance citizens' lifestyle (Aldairi & Tawalbeh, 2017). Examples of Smart City solutions are smart transportation systems, smart parking and smart buildings (Shim et al., 2019). The Smart City is designed, constructed and maintained by using highly advanced integrated technologies that are linked with computerized systems comprised of databases, tracking and decision-making algorithms (Ijaz, Shah, Khan, & Ahmed, 2016). Even if several definitions of the Smart City concept have been proposed, there is still not a standard definition that has been adopted neither in empirical projects nor in theoretical research (Negre, Rosenthal-Sabroux, & Gascó-Hernández, 2017). However, all the definitions agree on that a Smart City is an urban space that tends to improve the daily life of its citizens (Negre et al., 2017).

More than half of the world's population live in urban areas and a growing number of cities worldwide have started to develop their own smart strategies, with the use of private companies, for instance Cisco announced in 2017 a billion dollar investment in Smart Cities (Cui et al., 2018). The urbanization will increase, and the latest studies show that 60 % of the world's population will live in urban environments by the year 2030 (Aldairi & Tawalbeh, 2017). This massively growing population in urban environments have led to the need of advanced management and techniques to make the cities smart and be able to handle all the people in the cities (Ahvenniemi, Huovila, Pinto-Seppä, & Airaksinen, 2017; Aldairi & Tawalbeh, 2017). Smart Cities also aim to handle the challenges that face the globe with climate changes, limited resources and high population growth as the culprits of the challenges (Aldairi & Tawalbeh, 2017). Cities have a key role in fighting against the climate change and the development of new smart technologies is seen as a key factor in decreasing greenhouse gas emissions and improving energy efficiency of cities (Ahvenniemi et al., 2017). In addition, Smart Cities aim to secure economic competitiveness in urban spaces and let urban citizens experience classier lifestyles (Aldairi & Tawalbeh, 2017).

Although the Smart City creates new economic and social opportunities for the cities and their citizens, Smart Cities also pose challenges to security and expectations of privacy (Elmaghraby & Losavio, 2014). Security and privacy concerns arise since Smart City applications not only collect sensitive information about the citizens but also control important infrastructures in the city and influence people's lives (Zhang et al., 2017). According to Khatoun & Zeadally (2017) Smart Cities are exposed to a diverse set of cyber security threats and criminal misuses. A single Smart City vulnerability can put the entire city at a risk when exploited by an individual or organized criminal group (Khatoun & Zeadally, 2017). Cities and their infrastructure are already very complex structures and interweaving them with complex Smart City solutions, reliant on wireless sensor networks and integrated communications systems makes them vulnerable to power failure, software errors and cyberattacks (Edwards, 2017).

In a Smart City security concerns exist. For instance 1) Internet of Things (IoT) which incorporates a number of heterogeneous devices, and gives access to information of various online services in Smart Cities, 2) smartphone apps, which provide services of smart mobility, take mobile data, use trace-analysis and data mining techniques and 3) individuals of Smart Cities use different services and communicate with each other through technologies that are connected using heterogeneous systems and networks that are targets for hackers who wants to intrude their personal privacy (Ijaz et al., 2016). Malware infections, data breaches and cyberattacks on cyber physical systems are incidents that show an up warding trend, and from 2005 until 2017 and more than 7000 data breach incidents were made public (Sen, 2018). These breaches resulted in that more than one trillion individual records were being compromised (Sen, 2018). In order to ensure the continuity of critical services in a Smart City the information security and privacy must be guaranteed (Ijaz et al., 2016). In this thesis, we focus on the information- and cybersecurity (hereafter security but distinguished from physical security) and privacy challenges in Smart Cities and in what ways the Smart Cities handle and tackle these challenges.

1.2 Problem area

Smart Cities have many potential advantages, like easing the lives for patients that needs health services at home (Solanas et al., 2014) and improve mobility by making it a seamless system of green, efficient and flexible transportation to meet citizen’s needs (Docherty, Marsden, & Anable, 2018). To achieve these advantages Smart Cities must protect individual privacy and security in order for the citizens to use the Smart City systems (Braun, Fung, Iqbal, & Shah, 2018). The citizens must be confident and secure to use the Smart City systems as intended because without the citizens participation the Smart City is obsolete (Braun et al., 2018).

Smart applications are exposed to high security and privacy risks due to the heterogeneity, scalability and dynamic characteristics of IoT systems, compared to conventional computing systems (Cui et al., 2018). A Smart City is vulnerable to a number of security attacks because of the heterogeneous nature of resource constrained devices (Biswas & Muthukkumarasamy, 2016). In a Smart City the attack surface is extended, because of the several interconnected cyber physical components, infrastructures and users (Popescul & Genete, 2016). Breaches of security and privacy can provoke the compromising of entire systems and an infection can be easily transmitted between systems (Popescul & Genete, 2016). This could lead to an infection of the city itself by destroying the physical infrastructure and threatening lives (Popescul & Genete, 2016).

Most of the literature about Smart Cities promise and discuss the many opportunities and benefits with the Smart City, rather than the challenges that Smart Cities encounter (Bakıcı, Almirall, & Wareham, 2013; Edwards, 2017). Addressing existing challenges in certain areas becomes critical to achieve further improvement in the Smart Cities (Silva, Khan, & Han, 2018). The security and privacy concerns are more important in the Smart City than they are for any technological phenomena because of the increasing number of Smart Cities around the world (Aldairi & Tawalbeh, 2017). Many of the privacy and security threats already exist today but not as frequently as when these technologies become fully interconnected in the Smart City (Braun et al., 2018). There is also a threat of more damaging cyberattacks in coming years as intruders develop more sophisticated methods of hacking and the security measures will not be enough (Kitchin & Dodge, 2019). For example, the development of information technologies like machine learning and data mining have increased which leads to attackers becoming smarter and developing the ability to bypass attack detection mechanisms (Cui et al., 2018).

To problematize the area of security and privacy in the Smart City, security and privacy are rather reactively involved than proactively involved when Smart City initiatives become alive, and this becomes very problematic (Edwards, 2017; Popescul & Genete, 2016). Researchers as well as practitioners must pay closer attention to security and privacy challenges in Smart Cities, before the design and implementation phase of a Smart City is managed, due to the number of Smart Cities increasing worldwide that would increase the number of bad Smart Cities and security and privacy initiatives

(Aldairi & Tawalbeh, 2017). For these reasons, it is of importance to investigate in what ways Smart Cities actually work with security and privacy challenges in their Smart City, and in what ways they apply security and privacy in the process.

1.3 Research question

Identifying the need to investigate how security and privacy are tackled in Smart Cities, this thesis tackles the following research question:

- In what ways do Smart Cities work with security and privacy challenges?

“In what ways” concerns, in this thesis, what possible solutions Smart Cities apply in respect to the security and privacy challenges that they encounter. The research question does not include the word solutions because the interpretation that all Smart Cities have solutions to security and privacy challenges should not be made from our point of view.

1.4 Purpose

The primary purpose of this thesis is to investigate in what ways Smart Cities work with security and privacy challenges. However, to investigate in what ways Smart Cities work with security and privacy it becomes important to first determine the challenges faced in a Smart City concerning security and privacy.

The number of papers about Smart City security and privacy is still limited (Cui et al., 2018), while also knowing that Smart City design, implementation and application has been evolving in recent years, this thesis challenges the way Smart Cities work with security and privacy. By focusing on the fact that Smart Cities often forego security and privacy in the early stages of its development, making it difficult for Smart Cities to apply decent security and privacy solutions that would reduce their challenges related to them. To summarize, it is thus particularly interesting to investigate in what ways Smart Cities work with security and privacy because the focus in Smart Cities have been on the rollout of technologies while there have been a loss of focus on the security and privacy when implementing Smart City solutions (Kitchin, 2016).

1.5 Delimitation

This thesis will focus on investigating in what ways Smart Cities work with security and privacy challenges. Therefore, the study is delimited to only the security and privacy challenges in a Smart City and the research will not investigate any other challenges related to Smart Cities. This thesis will not give a full-scale description of *how* Smart Cities work with security and privacy challenges or give a full-scale solution of how to implement Smart City initiatives in a secure way.

This study is limited to the cyber- and information security and privacy, these are the primary concerns in Smart Cities related to security and privacy because of the advanced integrated technologies and systems that Smart Cities possess (Ijaz et al., 2016). Physical security is another type of challenge that is beyond the scope of this study and it will not be investigated.

2 Literature review

In chapter 2 the key literature that shape the foundational basis of this thesis is presented. Under paragraph 2.1 and 2.2, the concepts of the Smart City, information security, cyber security and privacy are presented. Paragraph 2.3 presents the security challenges and 2.4 presents the privacy challenges in a Smart City. Paragraph 2.5 and 2.6 describe the consequences of these challenges and possible solutions. These three (2.3, 2.4, 2.5 & 2.6) paragraphs create the four concepts that are the basis for the analysis of empirical results. The next paragraph, 2.7, presents our literature review summary and paragraph 2.8 contains our research model, which helped form a basis for the data collection.

2.1 The Smart City concept

A Smart City can be defined in various ways, due to that the idea of Smart Cities is evolving, the concept is very broad and every city is unique (Manville et al., 2014). There is also an overlap of the Smart City concept with related city concepts (Manville et al., 2014). Smart Cities can be considered as knowledge cities, intelligent cities or sustainable cities (Cocchia, 2014). The concepts are interconnected, and the concepts often share similar sustainability goals (Ahvenniemi et al., 2017). However, during the last years, there has been a shift in cities striving for Smart City incentives (Marsal-Llacuna, Colomer-Llinàs, & Meléndez-Frigola, 2015).

There is also a generous variety of Smart City definitions (Ahvenniemi et al., 2017). The concept is widely used today but there is still not a clear and consistent understanding of its meaning (Ahvenniemi et al., 2017). Countries, governments and cities decide the concept of Smart City by themselves regarding of how far they will go for smartening the city according to their willingness to change the city, their financial situation and resource limitations (Aldairi & Tawalbeh, 2017).

A Smart City is the collaboration between governance institutes and private and public companies that implement and use long-term computerized platforms that enforce using modern technologies (Aldairi & Tawalbeh, 2017). The idea of the Smart City is grounded in the development and connection of social capital, human capital and information and communication technology (ICT) infrastructure to create an improved and more sustainable economic development and a greater quality of life for the citizens (Manville et al., 2014). In the Smart City there are five central components that are necessarily required, and these are; 1) modern information and communication technologies, 2) buildings, 3) utilities and infrastructure, 4) transportation and traffic management and 5) the city itself (Aldairi & Tawalbeh, 2017). Smart Cities have further been defined along six dimensions (Manville et al., 2014). The six dimensions where the cities can become smarter are smart governance, smart economy, smart people, smart mobility, smart living and smart environment (Khatoun & Zeadally, 2016; Manville et al., 2014).

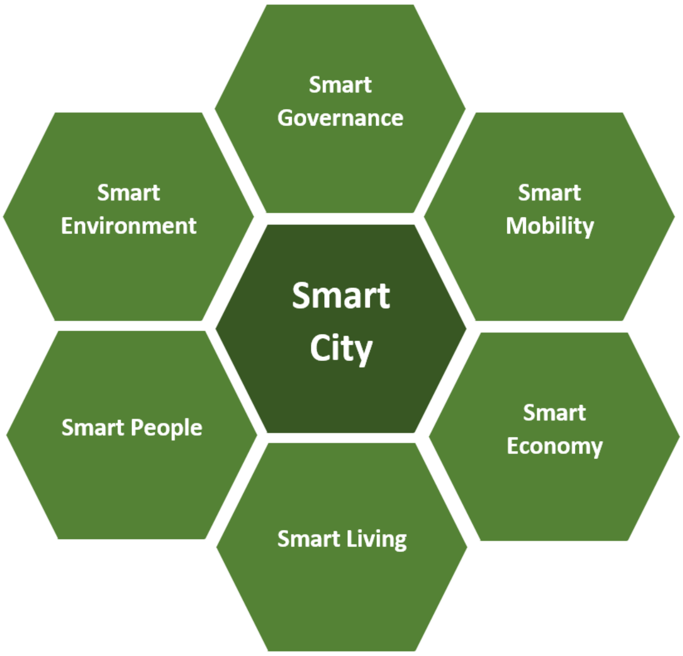


Figure 2.1. Dimensions of the Smart City

Smart governance is characterized as the capability of governments to make improved decisions through the combination of ICT tools and collaborative governance and is considered as a basis for developing smart government (Pereira, Parycek, Falco, & Kleinhans, 2018). Smart governance is the use of data, people, and other resources to enhance decision making and deliver results that meet the needs of the citizens which could improve quality of life (Pereira et al., 2018). Smart Governance is also the intersection of the six main Smart City dimensions (Pereira et al., 2018). Kitchin (2016) describes that smart government is produced by enabling new modes of operational governance, improved models and simulations to guide future development, new forms of e-government, informed decision making, and making governments more transparent, participatory and accountable (Kitchin, 2016).

Smart mobility is about traffic, transportation and logistic systems according to Aldairi & Tawalbeh (2017). Smart mobility is produced by creating intelligent transportation systems and efficient public transport (Kitchin, 2016). Transport today produces several negative impacts and problems for the quality of life in the cities like street congestion and pollution and can have a negative impact on the citizens work and life balance (Benevolo, Dameri, & D'Auria, 2016). Smart mobility is therefore one of the most promising facilities in the Smart City because it could produce several benefits for the quality of life for almost all stakeholders in the city (Benevolo et al., 2016). The most important smart mobility objectives are reducing pollution, reducing traffic congestion, increasing people safety, reducing noise pollution, improving transfer speed and reducing transfer costs (Benevolo et al., 2016).

Smart economy is about e-commerce, e-business, production and is produced by fostering entrepreneurship, production and competitiveness (Kitchin, 2016). Smart economy has been associated with the presence of industries in the field of ICT or employing ICT in production processes (Albino, Berardi, & Dangelico, 2015). Smart economy also entails local and global interconnectedness and international embeddedness with physical and virtual flows of goods, services and knowledge (Manville et al., 2014).

Smart people include e-skills, ICT-enabled working, access to education and training, human resources and capacity management (Manville et al., 2014). Smart people are produced by creating more informed citizens and fostering creativity, inclusivity, participation and empowerment (Kitchin, 2016).

Smart environment include energy, water, waste management, clean environment and controlled pollution (Aldairi & Tawalbeh, 2017). Smart environments are produced by promoting sustainability, resilience and the development of smart energy (Kitchin, 2016). Smart energy includes renewables, ICT-enabled energy grids, green buildings and green urban planning (Manville et al., 2014).

Smart living is about improving quality of life and a classy lifestyle, increasing safety and security and reducing risks, reasonable consumption and stable behavior (Kitchin, 2016). In addition to this Manville et al. (2014) describe that smart living incorporates good quality housing and accommodation and that smart living is linked to high levels of social cohesion and social capital.

2.2 Information security, cybersecurity and privacy

The concepts of information security, cybersecurity and privacy are presented here since they are essential to answer the research question.

2.2.1 Information security

The aim of information security is to ensure business continuity and minimize business damage by limiting the impact of security incidents. Information security incidents damage organizations' reputations, they are costly and disrupt operations and because of breaches, information security is the CIO's top priority (McLaughlin & Gogan, 2018). Information security can be defined in several ways and the international standard defines information security as the preservation of the confidentiality, integrity and availability of information (Von Solms & Van Niekerk, 2013). Information security is not a product or a technology, but a process and it should be introduced as a process from the design phase through the development lifecycle (Kajtazi, Vogel, Bugeja, & Varshney, 2018). Since the usage of computers and networks have evolved, the process of securing these computers and networks also evolved to extend beyond only the technical aspects (Von Solms & Van Niekerk, 2013). Information security can also be defined as the protection of information and its critical elements which includes the hardware and systems that use, store and transmit that information (Whitman & Mattord, 2011). Whitman & Mattord (2011) identifies critical characteristics of information that gives value in organizations, these include confidentiality, integrity and availability of information but are not limited to only these. These three are known in information security as the CIA triangle and the security of these three characteristics of information is important but today, these three alone do not adequately address the constant changes of the computer industry environment. Due to this the authors (Whitman & Mattord, 2011) add authenticity, utility and possession to the list of information characteristics that needs protection.

Traditionally, a good security practice was often achieved through some effective efforts that intended to ensure the CIA-triad but Smart Cities, that are characterized by the use of IoT systems, have aspects that are not covered by this model (Kajtazi et al., 2018).

2.2.2 Cybersecurity

In today's information age, cybersecurity is one of the most crucial concerns (International Telecommunication Union, 2017). Information security and cybersecurity are in many publications used interchangeably and they are similar in many cases but Von Solms & Van Niekerk (2013) discuss that there are cybersecurity threats that do not form part of the formally defined scope of information security. Three of these scenarios are home automation, cyberbullying and digital media.

Information security is defined as the assets that need to be protected, these include all aspects of the information itself. It also includes the protection of the underlying ICT assets and then it goes beyond the technology to include information that is not stored or communicated directly using ICT (Von Solms & Van Niekerk, 2013). In cybersecurity, on the other hand, the assets that need protection can range from the person her/himself to common household appliances, to the interests of society at large. These assets actually include anything or anyone that can be reached via cyberspace. The term cybersecurity is related with information security, but not analogous (Von Solms & Van Niekerk, 2013). The most defining characteristic of cybersecurity is the fact that all assets that should be protected also needs protection because of the vulnerabilities that exists as a result of the ICT that forms the basis of cyberspace Von Solms & Van Niekerk (2013). International Telecommunication Union (2008) defines cybersecurity as "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (International Telecommunication Union, 2008, p.2).

Cybersecurity is a crucial component that should be considered when using computing technologies (Reddy & Rao, 2016) and cybersecurity of nations is a critical challenge which affects the basic functioning of a society as well as the economy (Subramanian, 2016). The importance of cybersecurity is increasing due to that cybersecurity incidents will increasingly impact software, hardware, national infrastructure, social life, defense and the daily operations of organizations and individuals (Sen, 2018). Smart Cities are exposed to various sets of cybersecurity threats and a single Smart City vulnerability, when utilized by an organized group or individual, can put a risk to the entire city (Baig et al., 2017).

2.2.3 Privacy

To selectively reveal oneself to the world is a human right in many jurisdictions and privacy is a state that a lot of people value (Kitchin, 2016). Although, privacy is understood differently between cultures and contexts, both as an everyday and legal concept. But in general terms, privacy concerns acceptable practices with considerations on the accessing and disclosing of sensitive and personal information about a person (Kitchin, 2016). There is also an intersection between security and privacy and a badly secured system can lead to privacy violations, for example when attacks happen that take control of devices that affect people's lives (Kajtazi et al., 2018). Situations can also happen when privacy becomes a cause for concern for the security, for instance when strengthening surveillance systems for a better security (Kajtazi et al., 2018). Vattapparamban, Güvenç, Yurekli, Akkaya, & Uluağaç (2016) describe the use of drones for Smart Cities as a tool that can violate the privacy of people since it is easy to install a camera or another device on it to collect information. It is argued that drones will take a major role in future Smart Cities because they can deliver mobile hot spots, deliver goods and maintain surveillance but the privacy and cybersecurity challenges also need to be addressed (Vattapparamban et al., 2016).

In the past decade, because of the growing dependence of private and public institutions on digital interactions with citizens and consumers, privacy research has increased rapidly (van Zoonen, 2016). Privacy has been identified as a key policy, regulatory and legislation challenge of the 21th century by various national and international organizations (van Zoonen, 2016). This can be a result from the reports of security breaches that can be seen daily in news sources and that the number of cyberattacks worldwide increased with 25% in 2013 (Presley & Landry, 2016). In 2014, hackers got hold of addresses, emails, names and phone numbers of 76 million households and 7 million small businesses by compromising around 90 of JPMorgan's servers (Karyda & Mitrou, 2016). InfoWatch Analytical center registered 1395 cases of data leaks in 2014, where 410 million personal data records had been endangered due to external attacks (Karyda & Mitrou, 2016). These are examples of when security breaches happen that affect the individual's privacy. A data breach, which often is a result of external hackers, deprive people of their right to confidentiality, privacy and integrity of their personal information (Karyda & Mitrou, 2016). Khatoun & Zeadally (2017) describe that security is needed to be taken into serious consideration due to users' privacy and the safety of human life.

The research on people's privacy concerns is diverse in terms of theory but two important paradoxes have been identified, concern and behavior. These two together are known as the privacy paradox. These two paradoxes explain how people perceive different services depending on how they affect them and their privacy (van Zoonen, 2016). For this thesis, the focus will be on security challenges and how security breaches can affect city and the citizen's privacy because without sufficient privacy and security protections, users may abstain from accepting the Smart City (Zhang et al., 2017). Elmaghraby & Losavio (2014) also describe that privacy protecting systems are technological challenges that go hand-in-hand with the continuous security challenges.

2.3 Security challenges in the Smart City

Braun et al. (2018) write about security and privacy challenges and they describe that security as a concept is a dynamic and genuine attempt to avert harm to the Smart City and its citizens, both directly and indirectly through physical and digital connections. Edwards (2017) describes security challenges as the susceptibility of data to either deliberate or accidental breaches as a result of technical or organizational failures. The technology is a key factor in order to provide better services to the government and the citizens and to fulfill the promises of a Smart City functional (Ijaz et al., 2016). Thus, a Smart City is not so smart if the concerns in security are not properly delivered (Ijaz et al., 2016).

Internet of Things

The Internet of Things (IoT) has resulted in numerous new smart technologies and represents an instrumental factor in creating and maintaining the services of a Smart City, hence making the challenge of secure information flow a big role with respect to it (Shim et al., 2019). Baig et al. (2017) discuss as well that IoT is the enabling technology in the Smart City and the Smart City includes several types of IoT sensors. The insecurity and vulnerability of Smart City systems is a widely acknowledged phenomenon which deduces from the known familiar lack of security and trustworthiness of the IoT in general (Ijaz et al., 2016). The data security is one of the negative issues with IoT (Shim et al., 2019).

The continued development of IoT-devices and the lack of security will also pose challenges in regards to privacy (French & Shim, 2016). Edwards (2016) discuss why the IoT devices are so insecure; IoT devices are normally cheap, small, without independent power source and historically made for industrial and not consumer use (Edwards, 2016). These devices are routinely designed with poor encryption strength and an absence of mandatory technical and security standards (Edwards, 2017). It is common that designers let the security aside when designing IoT applications according to Popescul & Genete (2016). The designers hope it could be added later-on and attack-resistance is normally losing against other design factors like good performance and low energy consumption (Popescul & Genete, 2016). According to a study by Smith & Miessler (2014) 70% of things in IoT enable an attacker to identify valid user accounts through account enumeration. Baig et al. (2017) present that confidentiality and integrity compromise, eavesdropping, data loss, availability compromise and remote exploitation are some of the security threats to IoT sensor.

Smartphones

Smartphones are an important component of the IoT infrastructure in a Smart City because they give access to various services and applications that help in maintaining and creating a better Smart City (Ijaz et al., 2016). Shim et al. (2019) state this as well and discuss that the smartphone improves the citizens everyday life. The smartphones are also the main source of people's involvement in the Smart City. Because the smartphones have become very popular in the last years it has also made them an attractive thing to be attacked by hackers and viruses (Ijaz et al., 2016). The main security threats in smartphones are malicious smart applications, botnets, spyware, threats from Bluetooth, location and GPS (Global Positioning System), threats through Wi-Fi and threats in social networks (Ijaz et al., 2016).

Smart grids

Smart grids are another important part of the Smart City regarding energy deployment and management (Ijaz et al., 2016). Smart grids are used to communicate data in real time and when the data is shared in real time scenario among power generators, distributed resources, service providers and users, any information that is prone to attacks could take the system to failure (Ijaz et al., 2016). According to Cui et al. (2018), the smart metering infrastructure used in smart grids can monitor the lives of citizens, that includes their living habits and working hours. The smart grid would be a prime target for cyber-attacks in the Smart City and power failures can have serious economic and psychological consequences on the attacked city or country (Goel, 2015).

Baig et al. (2017) describe that smart grid threats can be categorized into those that affect network availability, data integrity and information privacy. Ijaz et al. (2016) describe that these three threats, and also threats to devices, should be kept under consideration while constructing and deploying a smart grid in the Smart City. The smart grid maintains a two-way communication channel with multiple intelligent smart devices and the cloud (Baig et al., 2017). These multiple exposed devices create numerous entry points for an adversary to penetrate the smart grid and also expose smart grid data stored in the cloud to various security threats (Baig et al., 2017). An adversary can for instance extract household information such as the number of people living in the house, consumption patterns and types of appliances in use (Jokar, Arianpoo, & Leung, 2016). According to Goel (2015) the smart grid is vulnerable to data spoofing attacks, including transmitting false data, disabling relays, disrupting load balance and inducing faults.

Cloud services

Cloud services will be needed in a Smart City to store vast amounts of data (Braun et al., 2018). Baig et al. (2017) also mention that the cloud will be used for centralized data storing in the Smart City. The Smart City can also take a comparative advantage of powerful cloud servers for data storage and processing the information (Zhang et al., 2010). There are multiple suppliers of cloud services that can help Smart Cities evade limitations imposed by physical memory and computing power. Even though there are benefits with cloud services and cloud storage, they also pose challenges (Braun et al., 2018). Zhang et al. (2010) discuss that the cloud services face security threats due to the untrusted cloud servers. Cloud service providers can also complicate matters by adding additional practices and standards for security and privacy. Also, when these providers handle extensive amount of confidential information, questions about consent and responsibility in a Smart City can be brought up (Braun et al., 2018). For instance, questions like: 1) when Smart Cities allow third parties to store, handle and manipulate raw confidential data, are user’s privacy violated? and 2) who would be held responsible for a data breach in the cloud storage system?

Baig et al. (2017) also discuss the challenges with cloud providers and that the Smart City has little control on the management and security. When deploying on a community or public cloud, for instance, the control of data is delegated to the infrastructure owner to make sure that an adequate security policy are being executed to ensure that risks are reduced (Zissis & Lekkas, 2012). Cloud security is a challenge for Smart Cities because when the smart networks store personal data and the data is used in eternity without transparency the citizens in a Smart City may call for a conventional government intervention or resist using the Smart City services (Braun et al., 2018).

Artificial Intelligence

Threats of artificial intelligence is one of the challenges that Braun et al. (2018) present that is worth pointing on. AI systems play indispensable roles in smart applications such as home appliances and pacemakers (Cui et al., 2018). A Smart City will most probably rely on automation for efficiency and for implementing automation, artificial intelligence will be critical in a versatile manner (Braun et al., 2018). Anything from identifying malevolent behavior inside the Smart City network, to connecting citizens to emergency services when they are in need, will depend on artificial intelligence to identify problems and implement solutions at a velocity that surpasses human ability (Braun et al., 2018). As it is shown, AI systems play essential roles in many smart applications like, for instance, automatic control of trading systems, pacemakers and home appliances which are systems that constitute physical threats if they are attacked by hackers (Braun et al., 2018). At the same time as AI is evolving, attackers are also getting smarter about the AI technology and they might understand how machine learning protection mechanisms were designed or trained so they can adopt approaches to weaken the training effects, and to reduce reliability of the algorithms (Cui et al., 2018). Due to this, the question arises about what happen if the artificial intelligence system is compromised (Braun et al., 2018).

Cyberattacks

Cyberattacks try to change, destroy, or disrupt computer systems, programs or networks resident in transmitting these systems, programs or networks (Owens, Dam, & Lin, 2009). Against operational systems there are three forms of cyberattacks that could happen. Availability attacks seek to shut down a system or deny access to it, confidentiality attacks seek to monitor activity or extract data and integrity attacks seek to enter a system to change information or settings (Singer & Friedman, 2014). Threats against cyber physical systems can target societally crucial systems, for instance systems that manage power grids, transportation networks and telecommunications networks (Sen, 2018). According to Cui et al. (2018), smart applications are exposed to hacking through up-to-date attacks like, for instance, spam attacks, eavesdropping attacks and identity attacks.

Cyberattacks on cyber physical systems have in the last years showed an upward trend (Sen, 2018). According to Kitchin & Dodge (2019) cyberattacks try to adventure one of the five considerable vulnerabilities of digital technologies that are essential to the Smart City systems. The first vulnerability is weak software security and data encryption. The second vulnerability involve the use of insecure legacy systems and poor ongoing maintenance. The third area of vulnerability is that Smart City systems are complex, large and diverse systems with many interdependencies and also with many attack surfaces (Kitchin & Dodge, 2019). This makes it hard to know what and how all components are exposed, and to ensure end-to-end security. The fourth vulnerability is that the interdependencies between Smart City systems and technologies can create cascade effects where extremely interconnected entities rapidly can transmit consequences to each other. The final vulnerability mentioned by (Kitchin & Dodge, 2019) is that there are multiple vulnerabilities issuing from human error and deliberate malfeasance of disgruntled (ex)employees.

Cyberspace is a goldmine of crime, violations and terrors, and attackers are also moving fast compared to defenses (Dorasamy, Haw, & Vigian, 2017). For instance, as smart grids start to rely more on sensors whose data are communicated over a communication network, they become vulnerable to attackers who can spoof sensor measurements (Sen, 2018). Examples of when cyber physical systems have been breached involves power blackouts in Brazil, the StuxNet computer worm and other industrial security breaches (Sen, 2018). Most cyberattacks today last no more than a few hours but even short-term disturbances can be an expensive disruption through lost productivity and opportunities and can also be life-threatening (Kitchin & Dodge, 2019).

Lack of security testing

A challenge related to the technical factors are that the governance authorities, which are the customers of the technology, do not test the security systems before they buy the technology based on the security factors (Ijaz et al., 2016). It is more important for the governance authorities to test the functionality than the security which is a bad prioritization (Ijaz et al., 2016). Edwards (2017) also discuss that most cities implement new technologies with little or no cyber security testing. This could lead to that, for example, traffic control sensors installed in cities can be easily attacked with a simple exploit programmed on cheap hardware (Edwards, 2017).

Lack of knowledge and awareness
Lee, Kim, & Seo (2019) discuss that one of the challenges with security in the Smart City is related to the staff's mistakes. Important information is leaked externally due to carelessness or lack of security awareness and knowledge of the employees (Lee et al., 2019). Harbers et al. (2018) discuss as well that there is a lack of knowledge and awareness among users, IoT producers and providers, and among the policy makers. This can result in cyber- and security threats (Harbers et al., 2018). Harbers et al. (2018) argue that there is a need of awareness of the challenges with the technologies in the first place to reduce the security risks.

Harbers et al. (2018) further state that when information systems become better protected by technological solutions, attackers shift their focus and attention to human elements to break into these systems. For instance, Shim et al. (2019) present that cyber- and security threats can happen because many users do not download and install security patches for their IoT devices in the Smart City. Human behavior can play a crucial role in mitigating cybersecurity risks and users are currently not protecting them as much as they could (Harbers et al., 2018).

Related to the lack of awareness is the unauthorized access (Lee et al., 2019). Threats of unauthorized persons accessing the system inside the Smart City without special authentication through vulnerable environments (Lee et al., 2019). The fast development and the complexity of IoT systems require a continuous update of knowledge and awareness for the users in order to stay well informed of the security challenges (Harbers et al., 2018).

2.4 Privacy challenges in the Smart City

Smart Cities combine the three greatest current threats to personal privacy; the IoT, big data and the cloud (Edwards, 2017). A lack of appropriate security in the Smart City systems can lead to a lot of privacy breaches and result in that sensitive information about someone can be accessed by unauthorized attackers (Zhang et al., 2017). Elmaghraby (2014) also describes that challenges in a Smart City can be categorized into technological-, security- and privacy challenges but these three areas are interrelated since the lack of security can be created by a technological limitation and this could lead to privacy breaches. Therefore, it is needed to present the privacy challenges in the Smart City.

Data sharing, data mining and mashup data
In a Smart City, privacy threats in data sharing and data mining exist. Interconnectivity is one characterizing factor in a Smart City so data will be transferred and utilized through the Smart City processes (Braun et al., 2018). This can lead to a variation in privacy standards due to different stakeholders taking advantage of the system (Braun et al., 2018). The use of smart systems in Smart Cities means that users need to offer their personal data to these systems and one of the most difficult challenge in a Smart City is to secure sensitive data (Li, Dai, Ming, & Qiu, 2015). Privacy threats in mashup data means that in a Smart City, data integration and data mashup increase the digital surface in a way which leads to that it provides more opportunities for security breaches (Braun et al., 2018). All the individual objects' that create a Smart City, for instance IoT objects, service platforms and smartphones, posture an alarming risk for the privacy of the Smart City when connections are made between the objects (Braun et al., 2018).

In a Smart City individuals use various services and communicate with each other through the latest technology that is connected using heterogeneous networks and systems which are the target for hackers who want to intrude their personal privacy thus depriving them from their personal right (Ijaz et al., 2016). The role of social networking should be considered regarding privacy and information security. When a smartphone is used, citizens can access internet through public Wi-Fi's, take online courses, pay their bill online and receive medical treatment, so the smartphone that use Smart City systems both stores and generates data (Li et al., 2015). The privacy concerns linked with the social networking depend on the level of identification of the provided information by the individual, the receivers and the way it may be used (Ijaz et al., 2016). Even if the social networking providers do not promise to expose their users identities, they can still provide required enough data to identify the individual's profile (Ijaz et al., 2016). Aldairi & Tawalbeh (2017) discuss that privacy is ensured by protecting five privacy related challenges: protecting identities that indicate protecting personnel and their confidential data; protecting people areas that indicate to protect each one's space and properties; protecting locations which indicate preventing spatial tracking; communication protection which indicate not to eavesdrop any kind of conversation and lastly transactions protection that protect every single purchase, exchange and query.

Location data

Smart City technologies radically expand the range, granularity and volume of the data being generated about people and places, and they capture data relating to all forms of privacy (Kitchin, 2016). Smart technologies have transformed location and movement tracking to a case where monitoring of location is pervasive, automatic, continuous and relatively cheap (Kitchin, 2016) and location data is the most frequently used data in smartphones (Li et al., 2015). It is easy to store and process data, and it is straightforward to create travel profiles and histories (Kitchin, 2016). These privacy harms raise significant challenges to existing approaches to protecting privacy (Kitchin, 2016).

Cities use different smart technologies to monitor and control activities, these technologies include, for instance: 1) sensor networks across street infrastructure, 2) CCTV cameras that track individual pedestrians, 3) GPS in vehicles and smart card tracking in buildings. The companies who own these technologies have a enormous amount of detailed spatial behaviour data from which many other insights can be indicated (Kitchin, 2016). Elmaghraby & Losavio (2014) also pointed out in their article that automobiles and their systems can be a great source of different kinds of data about a person's activities, especially now when GPS systems have become popular in vehicles. Elmaghraby & Losavio (2014) describe that locational data can detail a lot of a person's life that they do not wish to reveal.

Big data

Big data is related to the ideas of volume, velocity and variety and has come to the front for three reasons. These reasons are that the cost of storage and processing of data have dramatically fallen, algorithms for analysing enormous amounts of data have improved and the online data industries and IoT industries have created vast pools of data to mine (Edwards, 2017). Smart Cities are both consumers and producers of big data. Data is generated within traditional city infrastructure and utilities, which have become digital streams, and they are also complemented with big data generated from private companies (Edwards, 2017). Most of this data exist in silos today, but it will increasingly be combined by public city managers and private service providers (Karyda & Mitrou, 2016)

According to Demirkan et al. (2015) the two biggest fears humans have with big data is the security of this data and the personal privacy. Related to privacy, the key concerns around big data lies in: 1) the potential for reidentification of allegedly anonymized or pseudonymized data, 2) the lack of transparency on how results are obtained from big data, 3) the repurposing of big data collected for purposes that differs from the original, 4) the trend towards thorough collection of all the data and away from the principle by the Data Protection law that promotes minimization of data collection. It is not given that big data will involve personal data, but it constantly does and even when data is generated with seeming anonymity the ease of associating two large databases to identify people is well known by now (Edwards, 2017). Analytics which are based on information that derives from one or many IoT environments may enable the discovery of detailed information about an individual's life and behavior patterns (Edwards, 2017).

The public awareness of the loss of personal identifiable information through a breach in security have increased (Demirkan et al., 2015). Breaches of personal data have resulted in significant monetary, brand and consumer confidence losses (Demirkan et al., 2015). Securing big data is a leading concern and focus for security experts responsible for protecting a company's reputation and customer data and the governments protecting their city and citizens (Demirkan et al., 2015).

2.5 Consequences of security and privacy challenges

The Smart City commit to provide all the ways to maintain whole infrastructure and management challenges but if the technology is incorrectly implemented it can lead to attacks and frauds, and these can be very damaging to the core purpose of the Smart Cities. The attacks can cause even more damage and consequences than the benefits of the Smart City (Ijaz et al., 2016).

2.5.1 Critical systems

One of the crucial areas in the Smart City is the critical infrastructure where changing a single process in a system can cause problems or loss of services (Ijaz et al., 2016). This can happen in the critical infrastructures healthcare, industry and telecommunication (Ijaz et al., 2016). The healthcare sector is a paramount type of critical infrastructure as if it is prone to security threats it cannot just cause concerns about a patient's privacy but can also pose risks to a person's life as the critical information can be changed by the attacker (Ijaz et al., 2016).

Aldairi & Tawalbeh (2017) also discuss the security threats with the infrastructure in Smart Cities. First of all, Aldairi & Tawalbeh (2017) present the challenge that cities are full of private and public cameras, reaching these cameras and have access to them cause violation to individuals' privacy and spying on governmental concerns. Secondly, Aldairi & Tawalbeh (2017) discuss the threats against transport management systems and these systems face the most critical hacks as they cause catastrophes when they happen in air traffic systems or train control systems. Hacking traffic lights, road signs and speed limit signs could cause huge traffic jams and road accidents that will last for hours (Aldairi & Tawalbeh, 2017). The Smart City's critical infrastructure must therefore maintain its resilience, security and data integrity. Due to the damage that can affect Smart Cities and their promised services, critical infrastructure needs protection from malicious attacks (Ijaz et al., 2016).

Smart mobility may cause individual and location privacy concerns as personal information disclosure could happen in collecting, publishing and utilizing trace data (Ijaz et al., 2016). Some smartphone apps that provide services of smart mobility use mobile locations data for trace analysis and data mining techniques (Ijaz et al., 2016). The information sent and received from users' devices and are used in smart mobility infrastructure may subject to malicious attacks that could cause wrong traffic reports in satellite navigation systems. Lee et al. (2019) discuss that with traffic analysis, attackers can identify the behaviors and patterns of the operator by recording and analysing network traffic for a period of time.

One of the applications in the smart mobility is the traffic light systems in the Smart City. Traffic light systems have multiple vulnerabilities that can be exploited (Kitchin, 2016). Li, Jin, Hannon, Shahidehpour, & Wang (2016) discuss that if an attacker gets access to the network, they could also attempt to gain access to the controller. This could lead to that the attacker can eavesdrop on traffic and even control the traffic light (Li et al., 2016). It is therefore important to analyse the problems and threats in smart mobility and keeping in mind the security and privacy challenges (Ijaz, 2016).

In energy and utility optimization, data security and privacy are still top concerns (Ijaz et al., 2016). Disruption in the electric power operations can be catastrophic on national security and economy (Kitchin & Dodge, 2019) Technological advances can help reducing the deficiencies of current power and communication systems but can also lead to security breaches that are vulnerable to electronic intrusions. It can lead to unwanted switching operations that are executed by attackers which result in widespread power outages (Ten, Manimaran, & Liu, 2010). Intrusions can also happen in one or a few alteration and substations of the protective relay settings that can result in undesirable tripping of circuit breakers (Ten et al., 2010)

Smart communication includes the telecommunication sector, which is part of the critical infrastructure in the Smart City and is vulnerable to various attacks, frauds and privacy attacks through cyber security and data integrity (Ijaz, et al., 2016). The use of smartphone apps in smart communication may lead to data over-collection which can have consequences for the individual since it can be able for those who own the data to track people and their behaviours (Li et al., 2015). The security challenges related to that consumers do not download security patches can potentially put the entire internet in a city at a risk and this can lead to additional disruptions (Shim et al., 2019). For instance, various governance and financial activities are today handled through telecommunication and wireless networks, therefore the need of security and authentication even increases (Ijaz et al., 2016).

The banking and finance business is an important part of smart economy and a fundamental component of the Smart City. Thus, this component of the Smart City is the most vulnerable to security threats as it can be attacked for financial use (Ijaz et al., 2016). Cybercrimes, phishing, frauds and data integrity are four common security challenges in the banking industry within Smart Cities (Ijaz et al., 2016). Aldairi & Tawalbeh (2017) also mentioned spoofing as a security challenge in banking. The attackers could sabotage the economy of certain organizations or a whole city (Aldairi & Tawalbeh, 2017). So even if smart economy could promise better banking and business services in the city, it is a very vulnerable component of the Smart City (Ijaz, 2016).

2.5.2 Datafication

Kitchin (2016) present various privacy breaches that can happen in a Smart City environment and some of them can be an effect of a lack of appropriate security. Surveillance refers to watching, listening to or recording an individual’s activities. Distortion describes the dissemination of misleading or false information about individuals. Identification and aggregation mean that information is linked to particular individuals and that various pieces of data are combined about one person (Kitchin, 2016). With datafication can information be analysed in more sophisticated ways and make it possible to analyse across large data sets (Mai, 2016). This can lead to that information can be revealed about the user that the user had not thought of when the data is combined and analysed (Mai, 2016).

Tasks that previously were unmonitored or captured through a disciplinary gaze are now routinely traced and tracked through smart technologies (Kitchin, 2016). Because of this, detailed datasets are produced which are easily shared and can be joined to other datasets to extract additional insights. The results of this datafication is four with respect to privacy: 1) people are subject to greater levels of intensified inspection and modes of dataveillance and surveillance than ever before, 2) the pervasiveness of digitally-mediated transactions and surveillance, and the increasing use of unique identifiers to access services means that it is quite impossible to live an everyday life without leaving digital footprints, 3) the mass recording, storing, organising and sharing of big data about a phenomenon changes the uses to which data can be put, both for ill and for good, 4) this data allows a lot of deduction beyond the data that is generated to reveal insights that had never been depictured (Kitchin, 2016). According to Mai (2016) people reveal information both consciously and unconsciously as they perform daily activities. Even if people have provided information willingly, according to Mai (2016) it is common that people consent to provide personal information without much thought about it or without read or understood the consent form.

2.6 Solutions to security and privacy challenges

According to Kitchin and Dodge (2019) most strategies adopted for securing Smart Cities have mostly been technical mitigation solutions like access controls, encryption, security protocols, industry standards, staff training, and software patching regimes. Kitchin and Dodge (2019) discuss that the technical solutions have had some affect, but they propose that to secure Smart City systems require a wider set of systematic interventions that encompass mitigation, prevention, ensures enactment through both market-led initiatives, governance-led regulation and enforcement. In accordance with Kitchin and Dodge (2019), Kayworth & Whitten (2010) write that while technology is still essential for information security it represents just a part of an overall solution that must include other organizational elements of the business to create an effective information security.

There is no single solution for all the concerns related to the security and privacy challenges and Kitchin (2016) points out that rather a set of solutions is needed. Kitchin (2016) presents different ways of how to manage privacy and security concerns with respect to the Smart City and this paper will present the solutions in form of 1) technology solutions, 2) policy, regulatory and legal solutions and 3) governance and management solutions.

2.6.1 Technology solutions

Technology solutions to data security and privacy challenges consists of implementing best practice solutions in creating and maintaining secure Smart City systems and infrastructure (Kitchin, 2016). Standardization in itself can be a hard task in the Smart City environment due to the problems related to scalability and interoperability that implies IoT (Biswas & Muthukkumarasamy, 2016). Although, best practice solutions include, for instance: strong access controls, firewalls, strong end-to-end encryption, security certificates, up-to-date virus and malware checkers, isolation of trusted resources from non-trusted, ensuring that there are no weak links between components and ensuring full backup of recovery mechanisms and data (Kitchin & Dodge, 2019). According to Khatoun & Zeadally, (2017) 1) physical security for equipment, network cable and servers should be provided, 2) use of secure connection such as VPN for remote accesses is needed, 3) to secure any wireless network with WPA2 control is crucial and 4) deploying a firewall in every transition point is necessary to handle technical solutions. Presley & Landry (2016) also points on the importance of requirement of highly technical security controls such as firewalls, intrusion detection software and network segregation. The aim with these solutions is to reduce the attack surface (Kitchin, 2016).

Another technology solution is to develop effective Privacy Enhancing Technologies (PETs) and this is a continuous system of information and communication technology measure that protect privacy by reducing personal data (Kitchin, 2016). PETs increase individual control of PII (Personal Identifiable Information), minimise data generation, choose the extent of online linkability and anonymity of data, and track the use of one's individual data (Kitchin, 2016).

Due to the complexity of Smart City systems, where IoT devices are adopted at a great level, it is needed that the IoT systems is created with infrastructure that is pervasive, interoperable and intelligent at all system levels (Harbers et al., 2018). This includes the architectural, protocol and algorithmic levels (Harbers et al., 2018).

One more technology solution that Biswas & Muthukkumarasamy (2016) present is a blockchain based security framework to enable secure data communication in a Smart City. The benefits with blockchain is that it is resilient against many threats. The integration of blockchain technology with devices in a Smart City will create a common platform where all devices would be able to communicate securely in a distributed environment (Biswas & Muthukkumarasamy, 2016). In addition to this Shim et al. (2019) discuss that blockchain can provide a solution to the data security issues with IoT.

IoT on blockchain can reduce misinterpretations and fraud in the entire supply chain (Huh, Cho, & Kim, 2017).

2.6.2 Policy, regulatory and legal solutions

Policy, regulatory and legal solutions exponents the use of practical approaches which seek to address security and privacy harms and concerns (Kitchin, 2016). Next privacy by design, security by design, and education and training will be presented as a part of policy, regulatory and legal solutions.

Privacy and security by design

Privacy by design proposes that privacy is the default mode of operation and when collecting data, all data remains private unless the consumer explicitly said otherwise (Kitchin, 2016). Privacy is therefore hardwired into the design specifications and usage of business practices, information technology and physical environments. Privacy by design seeks to maximize both security and economic development, and not compromise one of them. Edwards (2017) describes privacy by design as an approach to protect privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure.

Privacy by design has been applied to the big data challenge in some way but in the IoT debates there is little sign of it (Edwards, 2017). The author (Edwards, 2017) describes that the most radical privacy by design solution to the IoT challenges could be to restrict that data collected by devices should be held and processed locally, under the control by the user, rather than given to data controller in the cloud (Edwards, 2017). This solution has received critique which includes that when processing is controlled locally in devices, code constraints can be built in that reify the rules of law protecting users (Edwards, 2017). According to Popescul & Genete (2016) the principle privacy by design is strongly recommended by the Alliance for Internet of Things Innovation (AIOTI). Privacy by design can also be used to obtain informed consent in IoT and Smart City environments and informed consent will most likely engender user trust (Edwards, 2017).

Security by design is complementary to privacy by design and it seeks to build security into systems, instead of layering it on as an afterthought (Kitchin, 2016). Because of this, it is necessary that security risk assessment is an essential part of the design process and that security measures are tested before the product is launched. Smart products and services should be design with security concepts in mind (Kajtazi et al., 2018). When security and privacy by design principles are utilized, mitigation measures should also be considered. Security is a continuous process and a plan for end-to-end security should be implemented and designed addressing all the components of an IoT ecosystem (Kajtazi et al., 2018).

Education and training

It is important to educate and train the users on how these technologies for handling privacy and security challenges work and to inform developers of their obligations and best practices. Kitchin (2016) favor four national education and training programmes. A general education programme that is directed at the public which sets out the security and privacy implications of Smart City technologies and what steps they can take to protect themselves against these harms is the first one. To complement this is an educational programme targeting school children that alert them about the data that is collected about them and how to manage their data privacy and security (Kitchin, 2016). The third programme are aiming at local authority staff that are in the development process of Smart City policy formulation, the acquisition of Smart City technologies, and the rollout and running of Smart City initiatives. The last is a training programme focusing on technology companies to set out their best practices and obligations that might give them a competitive advantage (Kitchin, 2016). Harbers et al. (2018) also discuss the importance of investments in education that, for instance, targets primary education, secondary education and universities since they are the future generations of users and developers of Smart City systems. Customized training is described to be more effective than generic training and informal peer training can improve employees' willingness to comply with security policies (McLaughlin & Gogan, 2018).

To raise awareness regarding IoT system challenges, risks and opportunities is needed through education and training (Kajtazi et al., 2018). Stakeholders such as regulators, policy makers and the general public should be included in this education since awareness and security education is needed for both developers and users of smart products (Kajtazi et al., 2018). Popescul & Genete (2016) also discuss that education is necessary to increase users' awareness and to protect confidentiality, integrity and accessibility of data in a Smart City.

To share cybersecurity information encourages firms to invest in cybersecurity related activities and it is argued that large firms are more engaged in sharing information compared to small firms (Yang, Kwon, & Lee, 2018). Yang et al. (2018) present that information sharing legislation has a positive effect of cybersecurity industries. Harbers et al. (2018) point on the need for awareness among users, producers and policymakers of the security and privacy challenges related to the technologies.

To sum up this section of solutions it is needed to point on that sufficient enforcement and monitoring are important when incentives related to security and privacy measures are implemented in a Smart City context (Harbers et al., 2018). To create effective standards, enforcement and monitoring is needed and to achieve adequate monitoring and enforcement it is important to invest in increased capacity at involved supervision authorities in Smart City environments (Harbers et al., 2018).

2.6.3 Governance and management solutions

Leadership and planning

To have strong principle-led governance and management is vital for creating a Smart City that wants to maximize the benefits of the concept and minimize the harms (Kitchin, 2016). Despite this, Smart Cities have been developed with little coordinated consideration of security and privacy harms. The initiatives have been slotted into existing city management with minimal strategic oversight (Kitchin, 2016). Presley and Landry (2016) implies that cybersecurity management is needed through the entire lifecycle and that it is a process where continuous security testing of the systems is needed. Presley & Landry (2016) indicate that cybersecurity risks are a concern for the project managers. Security audits, certifications and approvals are governance procedures that are needed to control and strengthen the implementation of IoT security (Kajtazi et al., 2018), which is a technology that characterize Smart City systems. It should be a requirement for the authorities to have an awareness and genuine concern over the security risks in the technologies that they buy and implement in the city (Ijaz, 2016).

McLaughlin & Gogan (2018) discuss how it is possible to prepare for information security incidents and one of them is to understand that information security is a moving target. Especially when technologies evolve, new risks arise with them, such as IoT and data being stored in the cloud. This means that people responsible over these areas are well informed and have solid evidence that new techniques are tested before deploying them (McLaughlin & Gogan, 2018). The authors (McLaughlin & Gogan, 2018) describes that training and incentives should be aligned with organizational norms, practices and culture since it can strengthen a security policy document. At the same time that this can strengthen employee's security awareness, it is also very hard to achieve a combination of complementary and aligned rewards, positive social influence and effective training.

To create incentives that copes with the complexity of the systems and to increase knowledge among stakeholders and users are crucial for the ones responsible of the Smart City initiatives. Incentives and objectives can include to strengthen the duty of care that can involve companies' duty to others and to provide privacy-friendly and secure systems (Harbers et al., 2018). Incentives related to supply chain responsibility can also help making a Smart City environment more secure since various parties are often involved in the creation of these systems (Harbers et al., 2018).

Given the potential harms that can arise, a more strategic and coordinated approach that consists of interference at four levels should be applied according to Kitchin (2016) and these are: Smart City advisory board, Smart City governance ethics and security oversight committee and core security/privacy team and computer emergency response team.

Smart City advisory boards

A Smart City advisory board is a high-level forum for the strategic visioning of the composition, form and ambition of its Smart City plan (Kitchin, 2016). The aim is to create a board that handles: how the evolving Smart City should unfold, the ethos and ethics underlying the Smart City agenda, the necessary governance and management structures, how it will align and shape the wider city development plan and the sourcing of necessary resources and finances, and the means to evaluate rollout and success (Kitchin, 2016).

Smart City governance, ethics and security oversight committee

The Smart City governance, ethics and security oversight committee (Kitchin, 2016) is more focused on operations than the advisory boards and their intent is to: 1) advise on the work priorities and programme, 2) oversee and audit the work of the privacy/security team, 3) certify that the city's Smart City strategies are being implemented and meeting targets and that they conform to legal and regulatory requirements, 4) ensure that response and mitigation plans and processes are in place, and 5) ensure there is clear communication to public concerning how the Smart City is being realised and how data are being generated, used, stored and shared (Kitchin, 2016).

Core privacy/security team

The core privacy/security team undertakes the work within the framework dictated by the governance, ethics and security oversight committee (Kitchin, 2016). The team's work includes: 1) liaising with the city departments and companies administering Smart City initiatives, 2) undertaking threat and risk modelling, 3) testing the security of Smart City technologies, 4) conducting Smart City ethics/ security assessments, 5) coordinating staff training on privacy and security challenges and 6) communicating Smart City policies to the public (Kitchin, 2016).

City computer emergency response teams

City computer emergency response teams (CERTs) are similar to emergency response teams that tackle city events. The team consists of key personnel that are drawn from IT services, the core privacy/security team, Smart City initiatives and emergency services (Kitchin, 2016). When a Smart City technology experience a cybersecurity incident, CERTs are handling the problem.

To finish this section of, it is of importance to point out that it does not exist a single solution to the security and privacy challenges in a Smart City but when the solutions are combined it is believed that a Smart City will become more secure. Therefore, all solutions will be investigated in our research.

2.7 Literature review summary

Table 2.1 below presents our results induced from the literature review, represented above in this section of the thesis. The table divides the findings into concepts, with introduction concepts, followed by concepts 1, 2, 3, and 4, further summarized by the main identified themes, with their identified subthemes. The supporting literature for each theme, followed by their sub-themes are also located in the last column.

Table 2.1: Literature review summary

Main theme	Sub theme	Supporting Literature
Introduction Concepts		
Smart City	Definition	Ahvenniemi et al. (2017), AlDairi & Tawalbeh (2017), Cocchia (2014), Manville et al. (2014), Marsal-Llacuna et al. (2015).
	Dimension of Smart City	Albino et al. (2015), AlDairi & Tawalbeh (2017), Benevolo et al. (2016), Khatoun & Zeadally (2016), Kitchin (2016). Manville et al. (2014), Pereira et al. (2018).
Security & Privacy	Information security	Kajtazi et al. (2018), McLaughlin (2018), Solms & Niekerk, (2013), Whitman and Mattord (2009).
	Cybersecurity	Baig et al. (2017), International Telecommunication Union (2008), International Telecommunication Union (2017), Reddy & Rao (2016), Sen (2018), Solms & Niekerk (2013), Subramanian (2016).
	Privacy	Elmagrahraby & Losavio (2014), Kajtazi et al. (2018), Karyda & Mitrou (2016), Khatoun & Zeadally (2017), Kitchin (2016), Presley & Landry (2016), Vattapparamban et al. (2016), Van Zoonen (2016), Zhang (2017).

Concept 1		
Security challenges in the Smart City	Internet of Things	Baig et al. (2017), Edwards (2016), French & Shim (2016), Smith & Miessler (2014), Ijaz et al. (2016), Popescul & Genete (2016), Shim et al. (2019).
	Smartphones	Ijaz et al. (2016), Shim et al. (2019).
	Smart Grids	Baig et al. (2017), Cui et al. (2018), Goel (2015), Ijaz et al. (2016), Jokar et al. (2016).
	Cloud services	Baig et al. (2017), Braun et al. (2018), Zhang et al. (2017), Zissis & Lekkas (2012).
	Artificial Intelligence	Braun et al. (2018), Cui et al. (2018).
	Cyberattacks	Cui et al. (2018), Kitchin & Dodge (2019), Dorasamy et al. (2017), Owens (2009), Sen (2018), Singer & Friedman (2014).
	Lack of security testing	Edwards (2016), Ijaz et al. (2016).
	Lack of knowledge and awareness	Harbers et al. (2018), Lee et al. (2019), Shim et al. (2019).
Concept 2		
Privacy challenges in the Smart City	Data sharing, Data Mining, Mashup data	AlDairi & Tawalbeh (2017), Braun et al. (2018), Ijaz et al. (2016), Li et al. (2015).

	Location data	Elmaghraby & Losavio (2014), Li et al. (2015), Kitchin (2016).
	Big Data	Edwards (2016), Demirkan et al. (2015).
Concept 3		
Consequences of security and privacy challenges	Critical systems	Aldairi & Tawalbeh (2017), Ijaz et al. (2016), Lee et al. (2019), Li et al. (2015), Li et al. (2016), Ten et al. (2010), Shim et al. (2019).
	Datafication	Kitchin (2016), Mai (2016).
Concept 4		
Solutions to security and privacy challenges	Technology solutions	Biswas & Muthukkumarasamy (2016), Harbers et al. (2018), Kajtazi et al. (2018), Khatoun & Zeadelly (2017), Kitchin (2016), Kitchin & Dodge (2019), Presley & Landry (2016). Shim et al. (2019), Huh, Cho, & Kim (2017).
	Policy, regulatory and legal solutions	Edwards (2016), Harbers et al. (2018), Kajtazi et al. (2018), Kitchin (2016), McLaughlin & Gogan (2018), Popescul & Genete (2016), Yang et al. (2018).
	Governance and management solutions	Harbers et al. (2018), Ijaz et al. (2016), Kitchin (2016), Presley & Landry (2016).

2.8 Research model

Based on the literature review and the literature review summary above we present a research model in order to guide the research process, see table 2.2. According to Biswas & Muthukkumarasamy (2016) it is important to identify the security and privacy challenges and their possible consequences in order to design an effective solution. Therefore, it is important to identify what the security and privacy challenges are and what this could lead to, to be able to understand in what ways Smart Cities work with security and privacy. The model includes four important concepts that are identified as crucial to answer the research question. The introduction concept identified in table 2.1 are not represented in the model presented in table 2.2 below, however, these are introduction concepts that are representable in every concept that are further used in this study.

Table 2.2: Research model

Concept 1: Security challenges	**Concept 2: Privacy challenges**
• Security risks with the technologies being used in the Smart City • Cyberattacks • Lack of security testing • Lack of knowledge	• Data sharing, data mining & mashup data • Location data • Big data
Concept 3: Consequences of security and privacy challenges	**Concept 4: Solutions to security and privacy challenges**
• Critical systems o Smart mobility o Energy and utility optimization o Smart communication o Banking and finance business • Datafication	• Technology solution • Governance and management solutions • Policy, regulatory and legal solution

The literature review, followed by the literature review summary and the research model, led us to our methodological choices. The next section presents not only our methodological position, but also how the research model influenced the design of our interview guide.

3 Methodology

This chapter arguments for the actions taken in the examination of the research problem. The chapter displays the interpretive approach, which is applied, and use interviews as the qualitative data collection technique. It argues for the selection of the three Smart City areas and selection of the eight respondents, and also the focus group. The process for developing the interview guide is described and the chapter explains how the coding was done using the tool NVivo. Ethical and professional standards was applied to all processes of these research to establish acceptable quality of the methods, instruments used, and results accomplished.

3.1 Research strategy

An exploratory research is appropriate to conduct when the goal is to scope out the extent of a phenomenon, problem or behavior and generate some initial ideas about that phenomenon (Bhattacherjee, 2012). Because of this, this thesis has an exploratory approach since the purpose with this paper is to investigate current security and privacy challenges and in what ways Smart Cities work with security and privacy challenges. The research question is *In what ways do Smart Cities work with security and privacy challenges?* and according to Järvinen (2008) what-questions can be used in most research strategies when it is part of an exploratory study.

To answer the research question, a qualitative approach is applied since a qualitative approach is the study of people and the social and cultural contexts in which they live, operate and behave (Recker, 2013), that fits well with the intentions of our study. Moreover, the qualitative approach is best suited to answer our research question since Smart Cities and in what ways they work with security and privacy challenges is both a social and cultural phenomenon. A qualitative approach most often consists of an interpretive research since the researchers develop interpretations of the data they collect and analyse (Recker, 2013), and therefore this thesis conducts an interpretive approach. To talk with respondents from Smart Cities that mostly are part of the preface of the different Smart City initiatives and to interpret on the data collected is necessary to answer the research question, and to investigate in what ways they work with security and privacy.

3.2 Data collection

To collect data, we used interviews. Interviews allows for the discovery of information that is important to participants that may not have been considered by the researchers and they are also appropriate for exploring sensitive topics (Gill, Stewart, Treasure, & Chadwick, 2008), which we consider the security and privacy topic to be. Interviews can be descriptive, exploratory or explanatory (Recker, 2013). We wanted to investigate in what ways Smart Cities work with security and privacy challenges and therefore we used descriptive interviews because they are used to provide a clear description of a phenomenon as perceived by individuals (Recker, 2013). In this way a subjective understanding could be generated (Recker, 2013). Focus is typically given to the development and exploitation of several individual perspectives regarding the subject to arrive at a comprehensive multi-faced description or conceptualisation (Recker, 2013).

Qualitative interviews can be unstructured, semi-structured, structured or in group (Myers & Newman, 2007). First of all, we had a group interview with a focus group with three experts on the subject of security and privacy in Internet of Things, smart homes and Smart Cities. We had the interview to find out what the problems in the area were according to them, and also to know that we focused on the right things and to test our interview guide. Recker (2013) recommend that the data collection procedures should be trained and tested beforehand. In addition to the group interview with experts in the subject, we used a semi-structured approach because semi-structured interviews are less intrusive and encourages two-way communication (Recker, 2013). Semi-structured interviews also have the advantages that they enable flexibility because new questions can be discussed during the interview as a result of what the respondents mention (Recker, 2013). Semi-structured interviews can also confirm what is already known while at the same time provide new information (Recker, 2013). This allows us to ask questions both based on our literature review and the respondents can in the same way present new information about in what ways they work with security and privacy challenges. According to Recker (2013) the respondent will not just answer the question but also give the reason for the answer which we consider essential to answer our research question.

3.3 Interview guide design

In the literature review a research model with fundamental concepts was created to guide the research process (see table 2.2). Based on this research model an interview guide was designed. To visualize the structure of our interview guide we based the development of the interview questions on the identified concepts of our research model presented in table 2.2, with concepts 1) security challenges, 2) privacy challenges, 3) consequences of security and privacy challenges and 4) solutions to security and privacy challenges. We believed that these concepts were crucial to answer the research question (see table 3.2). We also added introduction- and closing question to the interview guide.

We prepared the introduction of the interview in which we presented ourselves and the subject of the thesis to the respondent, like Myers and Newman (2007) propose. We started the interview by asking the respondent if he or she wanted to be anonymous in the thesis and if it was okay to record the interview. Bhattacherjee (2012) recommends recording the interview but only with the respondent's consent. Recording the interview made it easier for us to analyse the interview later. We had prepared some general introduction questions to start with since, according to Recker (2013), semi-structured interviews normally start with questions that are more general. We asked the respondent what they work with, what their responsibilities are and how long time they have worked with Smart City initiatives (see table 3.1). This helped us to better understand the respondent and the person's responsibilities. We then asked the respondent what a Smart City is according to them, because the concept Smart City has so many definitions it felt important to know that we had approximately the same definition as the respondent. We also asked what Smart City initiatives they have in the city. This helped us to understand how the city work with Smart City initiatives.

Table 3.1: Introduction questions in interview guide

Introduction questions
• Is it okay that we record the interview? • Do you want to be anonymous in the thesis? • What do you work with? • What are your responsibilities? • How long time have you worked with Smart City initiatives? • What is a Smart City according to you? • What Smart City initiatives do you have in your city?

Concept 1: Security Challenges
To get answers for concept 1, we asked questions relating to security challenges in their Smart City initiatives. To ask more general questions about security challenges in the Smart Cities was intended since we did not want to affect the answers of the questions and to see if the respondents mentioned something that was not discussed in the literature review. Furthermore, to ask questions about if the cities had received any cyberattacks was of interest due to if they had tackled them in different ways. Based on their answer from the question of what the security challenges are in their Smart City initiatives, we also wanted to investigate if they perceive any challenge greater than the other. We believed this was important to get an understanding of what security challenge they face in their Smart City initiatives.

Concept 2: Privacy Challenges
The second concept tackles the privacy challenges in a Smart City. We asked three broad questions for this concept which gave us the possibility to ask follow-up question when needed. The questions for the second concept was also constructed to be general since we wanted to see if the respondent's answers corresponded to what the literature review mentions.

Concept 3: Consequences of security and privacy challenges
The first and second concept led us into the third concept which is consequences of security and privacy challenges. To get answers that tackled the consequences was relevant according to what Biswas & Muthukkumarasamy (2016) mention, that it is important to identify security and privacy challenges and their possible consequences to develop an effective solution. The questions for the third concept are related to the first and second concept since we believe that many of them can be follow-up question to the questions under the first and second concept.

Concept 4: Solutions to security and privacy challenges
The questions under the fourth concept are a bit more structured than the questions under the first and the second concept. Because of our research question that wants to answer in what ways do Smart Cities work with security and privacy challenges, we believe that it is important to have more detailed and structured questions under this concept to ensure that our research question is being answered. However, we always started with a broad question of how they work with security and privacy in the Smart City and depending on their answers we asked more detailed questions. We wanted to ask questions related to management-, legal and policy-, and technical solutions since that is what our literature review brings up.

Table 3.2: Questions to concepts in interview guide

Concept 1: Security challenges	**Concept 2: Privacy challenges**
• What are the security challenges with Smart City initiatives in the city? • What are the biggest challenges for the security? • What are the hardest challenges to tackle? • Have you had any cyberattacks to the Smart City System?	• How do you think about privacy in the Smart City? • What are the risks with privacy in the Smart City? • How do you think privacy breaches can affect the Smart City systems?

Concept 3: Consequences of security and privacy challenges	Concept 4: Solutions to security and privacy challenges
Security: • What did the cyberattack result in? • What could this lead to in the city and the citizens? Privacy: • In what way can the security affect the privacy of the citizens? • Smart communication • Banking, finance and business • Datafication	• How do you work with security and privacy in the Smart City initiatives? o Management solutions? o Legal and policy solutions? o Technical solutions? • How do you stop cyberattacks? • What solutions are the most important ones? • Do you have any education or training about security? • Do you have any goals for handling the security and privacy? • Do you work with privacy by design or security by design? • What solutions take most time and resources? • Do you have any future plans for handling the security and privacy challenges?

We finished the interview with some closing questions (see table 3.3). We asked the respondents if they wanted to add something more that could be essential for us to know. We also asked for permission to follow-up the interview or if we could contact the respondent if we had any more questions, like Myers and Newman (2007) recommend. Lastly, we asked if the respondent knew or recommended anyone else that we could interview, by applying the snowballing technique (Myers & Newman, 2007).

Table 3.3: Closing questions in interview guide

Closing questions
• Do you want to add anything more that we have not talked about? • Is it okay for us to contact you if we have any further questions? • Do you know anyone else that could be relevant for us to contact?

3.4 Informant selection

In descriptive interviews the focus is to find several individual perspectives to arrive at a comprehensive multi-faced description (Recker, 2013). Therefore, we interviewed numerous people working with Smart City initiatives in different cities. We tried to find respondents at different positions in the cities to obtain divergent perspectives on in what ways they work with security and privacy, this is something Bhattacherjee (2012) recommends. It is also important that the respondents are selected based on their personal involvement with the phenomenon under investigation (Bhattacherjee, 2012). This is something we saw as important that the respondents had a position in projects with the right knowledge to be able to answer the interview questions.

To find the respondents we first needed to find cities that had Smart City initiatives. We wanted to interview respondents from cities with just a few Smart City initiatives in the first stages in the process to cities with at least one implemented Smart City initiative. This to be able to compare how they work with security and privacy in the Smart City. We used the maturity level table (see table 3.4) presented by Manville et al. (2014) for inspiration to see in what stages a Smart City could be in. We took the decision not to interview respondents from cities in maturity level one or maturity level two because they have no Smart City pilot testing initiative and have not implemented any Smart City projects yet.

Table 3.4: Maturity levels (Manville et al., 2014).

Maturity level	Description
Maturity level 1	A Smart City strategy or policy
Maturity level 2	In addition to level 1, a project plan or project vision but no piloting or implementation
Maturity level 3	In addition to level 2, pilot testing Smart City initiatives
Maturity level 4	A Smart City with at least one fully launched or implemented Smart City initiative

It was hard to determine in what maturity level the Smart City is in but after some research we found three suitable Smart City areas. From maturity level four we choose Copenhagen because we had some knowledge from before that Copenhagen was a city with many implemented Smart City initiatives, which also Manville et al. (2014) state. From maturity level 3 we choose Lund (Future by Lund, 2019b) and Malmö (Future by Lund, 2019a; Sensative, 2019) because they have a few pilot testing Smart City initiatives. It is unclear if Malmö and Lund have implemented any Smart City initiatives or if they are just pilot testing, due to that we can not make sure that they have fully implemented a Smart City initiative and will therefore represent maturity level three. We also choose Stockholm from maturity level three because they have a few Smart City initiatives and they also have the vision to be the smartest city in the world by the year 2040 (Landahl, 2017; Stockholms stad, 2017). This made Stockholm a very interesting city to see how they work with security and privacy challenges in their way to become the smartest city in the world. When the cities were decided we chose to split them into different areas, so Stockholm create one area, Malmö and Lund create another area and Copenhagen creates the last area. This because they collaborate together with the municipalities that are close to each other. It is important to point on that no research has been made in the latest years if these cities are in the exact maturity level as we describe but from what we have found we have made these interpretations.

When we had decided areas, we started to find respondents in these areas. In Copenhagen we had contact information to one person that work with the Smart City. To find respondents from Malmö and Stockholm we used the platform Smart City Sweden. In Lund we already had some contact information and we used the platform Future by Lund to find suitable respondents.

To contact the respondents for the interviews and ask if they wanted to participate in an interview, we first called the person to present ourselves and the subject of our thesis. We believed that it was more likely that the respondents would respond if we first called them and not just sent them an email. After calling the respondent we followed up the call by sending them an email to decide date and time. In the cases we could not reach the respondent by phone we just sent them an email. In some cases, the person we contacted knew someone that was better for us to interview and then they contacted that person directly or gave us their name and email so we could contact them. We also used the technique snowballing (Myers & Newman, 2007) because in some cases we asked the respondent in the end of the interview if they knew anyone else that they recommended us to interview. In this way we could find suitable persons that we were not able to find by ourselves, but we always took the decision by ourselves if this person was suitable for our research. The conducted interviews are presented below in table 3.5.

Table 3.5: Overview of conducted interviews

Appendix	Respondent number	Job title	Located in	Date	Duration	Language	Type of interview
1	Focus Group with E1, E2, E3	Researchers Malmö and Lund University	Lund/ Malmö	12.04.2019	50 min	ENG	Face-to-face
2	R1	Programleader Smart and connected city	Stockholm	16.04.2019	32 min	SWE	Skype voicecall
3	R2	Projectleader for Smart public environments, Future by Lund	Lund	18.04.2019	37 min	ENG	Face-to-face
4	R3	Senior Project Manager, Mobile Heights	Lund	24.04.2019	48 min	ENG	Face-to-face
5	R4	Smart City Program manager	Copenhagen	24.04.2019	43 min	ENG	Telephone voicecall
6	R5	Sustainable Business Hub	Malmö	25.04.2019	32 min	ENG	Face-to-face
7	R6	Security Coordinator Lunds kommun	Lund	26.04.2019	31 min	SWE	Face-to-face
8	R7	CIO Solna city	Stockholm	29.04.2019	32 min	ENG	Telephone voicecall
9	R8	Smart City and digitizingconsult Frederiksberg Municipality	Copenhagen	03.05.2019	35 min	ENG	Skype voicecall

3.5 Conducting the interviews

Interviews can be made either face-to-face, one-to-many, or via telephone/conference (Recker, 2013). Face-to-face interviews is the most typical form of interview (Bhattacherjee, 2012), we preferred to do the interviews face-to-face because it can be easier for the respondent to talk about sensitive subjects which the security and privacy aspects can be and we also wanted to see how the respondents reacted to different questions and topics. In the cases when we could not do interviews face-to-face, we used telephone or skype voice call to have the interview. We tried to use Skype conference call when the interviews were done by distance, to minimize the distance, but because of technical implications this was not possible. The telephone interviews and skype voice call interviews still gave us a good result.

In semi-structured interviews there is normally an incomplete script but the researchers could have prepared some questions but there is still space for improvisation (Myers & Newman, 2007). Semi-structured interviews are guided only in the sense that an interview protocol provides a framework for the interview according to Recker (2013). Before the interviews, we created an interview guide based on the literature review with topics and general questions about what we wanted to discuss with the respondent, as presented in paragraph 3.3. We decided to ask the same questions to all the respondents but depending on what they answered we asked different follow-up questions. Therefore, it is not exactly the same questions in all the interviews, but all the concepts have been tackled in the interviews.

We decided to not send the interview guide to the respondents before because we did not want them to prepare before the interview. We wanted to have an open interview. To make sure that we interviewed respondents with the right knowledge and that they were able to answer our questions we included some background information about us and the thesis when we sent them the email about the date and time for the interview. Based on that they could decide if they had the right knowledge.

Myers & Newman (2007) mention that lack of time is a problem that is common when qualitative interviews are conducted and to avoid this problem we made it clear for our respondents what the interview was going to be about and that they could be anonymous in our thesis if they wanted to. To risk that we didn’t have enough time we made sure that the respondents restrained at least 45 minutes because we believed that was enough time to answer our questions.

3.6 Data analysis

After the interviews were conducted the analysis process started. In qualitative research, it may not be productive to separate data collection and data analysis at the same extent as with quantitative research (Recker, 2013). Kvale (1996) describes that it is too late to start thinking about how the analysis of interviews should be done after they are conducted, and analysis should be thought about before they are conducted. This was thought of when designing our interview guide with the four concepts since these concepts were also going to be used when analysing and managing the data. It helped us when discussing the interviews directly after they were conducted, and it was also helpful in the interview situation since we had the concepts in mind which made it possible to analyse at the same time as the interviews were conducted.

3.6.1 Memoing

Before the transcription was done and directly after the interviews, we analysed them through a discussion about what just had happened and how it was achieved (Recker, 2013). This was meaningful for the analysis part since we could reflect on what just happened. It was helpful to give us guidance for the future research process (Recker, 2013).

3.6.2 Data transcription

Transcribing the interviews was the step after the interviews were conducted. The transformation or change from one form to another is the definition of transcribing (Kvale, 1996) and in this study, the transformation was from spoken language to written words. We used the tool Otranscribe to help us with the transcription since it was a useful tool that facilitated the process. To capture important observations from the interviews, one of us was the leader of the interview, who asked questions to the respondent while the other one analysed the respondent, took notes and gave input, this is in line with Bhattacherjee's (2012) recommendations. The transcription was done immediately after the interviews, to be able to have the interviews fresh in our mind and to add additional notes if it was needed. When the transcriptions were done, the transcriptions were checked by the other research partner to make sure that the phrases from the interview were perceived in the same way. When the interviews were conducted in Swedish, we decided to transcribe the interview in Swedish and after that translate the interview to English. According to Nikander (2008) transcripts bring clarity and transparency to the phenomenon under study by allowing the readers access to inspect the data on which the analysis is based. Therefore, we decided to translate our transcription so readers that do not understand Swedish could inspect the data on which the analysis is based.

Table 3.6: Overview of transcriptions

Appendix	Participant	Transcribed by	Checked by
1	Focus group	Amilia & Sofia	Sofia & Amilia
2	Ip1	Amilia	Sofia
3	Ip2	Sofia	Amilia
4	Ip3	Amilia	Sofia
5	Ip4	Sofia	Amilia
6	Ip5	Amilia	Sofia
7	Ip6	Sofia	Amilia
8	Ip7	Sofia	Amilia
9	Ip8	Amilia	Sofia

3.6.3 Coding of the transcriptions

When the transcription was done, we coded the data with the tool NVivo because we found it easy to search among all the data we had received from our interviews. NVivo is not suitable for every research but we believed it was helpful for this thesis to manage all data that was collected. NVivo is described as a good tool for data management but it should not be considered an analysis tool (The Triangle Admin, 2015) and therefore we used it to manage our data. We considered that NVivo was a useful tool for us since we had 8 interviews and one focus group interview which were all longer than

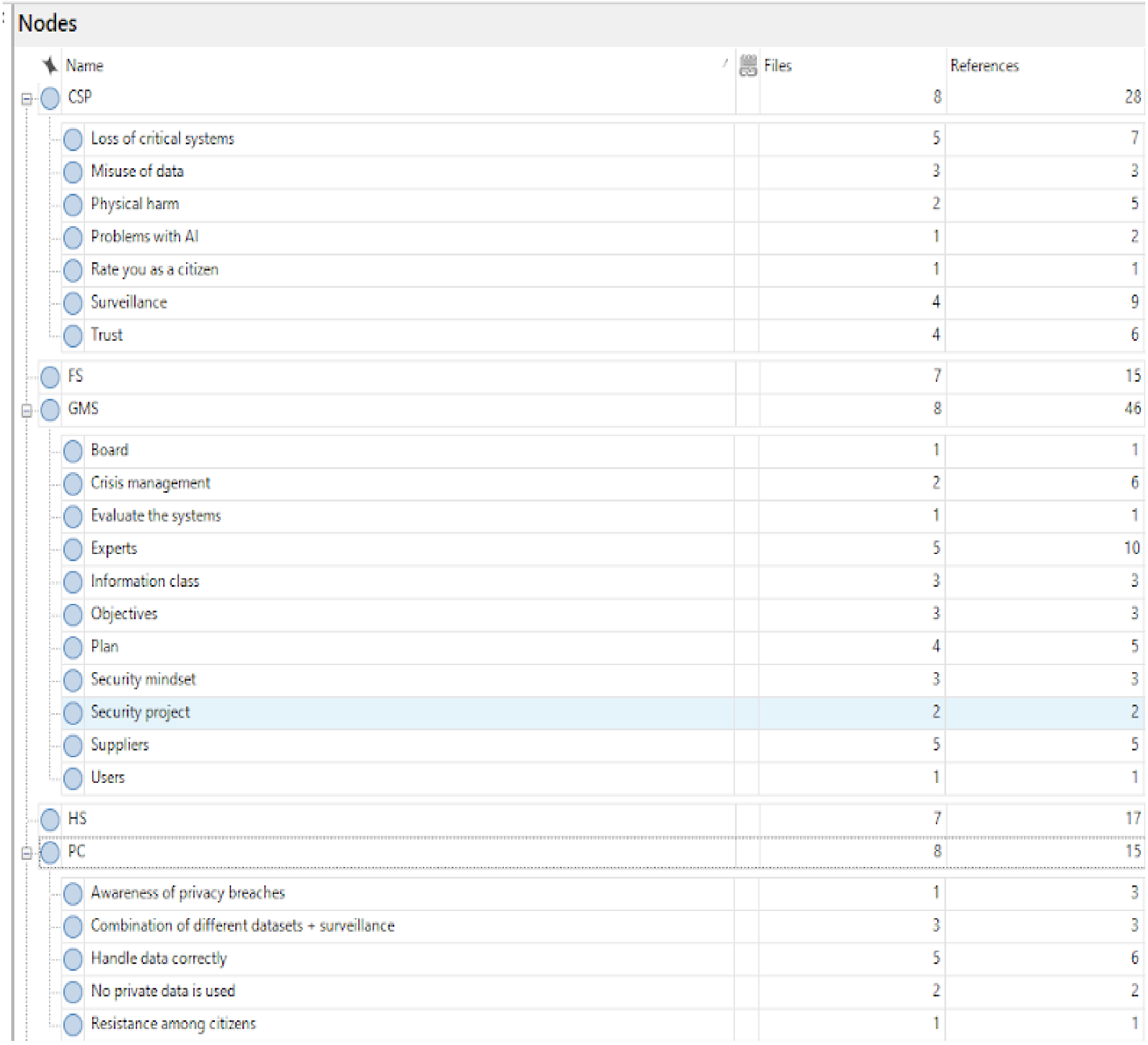
30 minutes (The Triangle Admin, 2015) which gave us a lot of rich data that NVivo helped us organise.

To create our base nodes in NVivo we used the concepts from the research model (table 2.2) but instead of having solutions as one node in NVivo the concept was split up into 1) TS, 2) RPLS, 3) GMS, 4) HS, 5) FS. All our base nodes and their description are presented in the table below (table 3.7).

Table 3.7: Base nodes with description

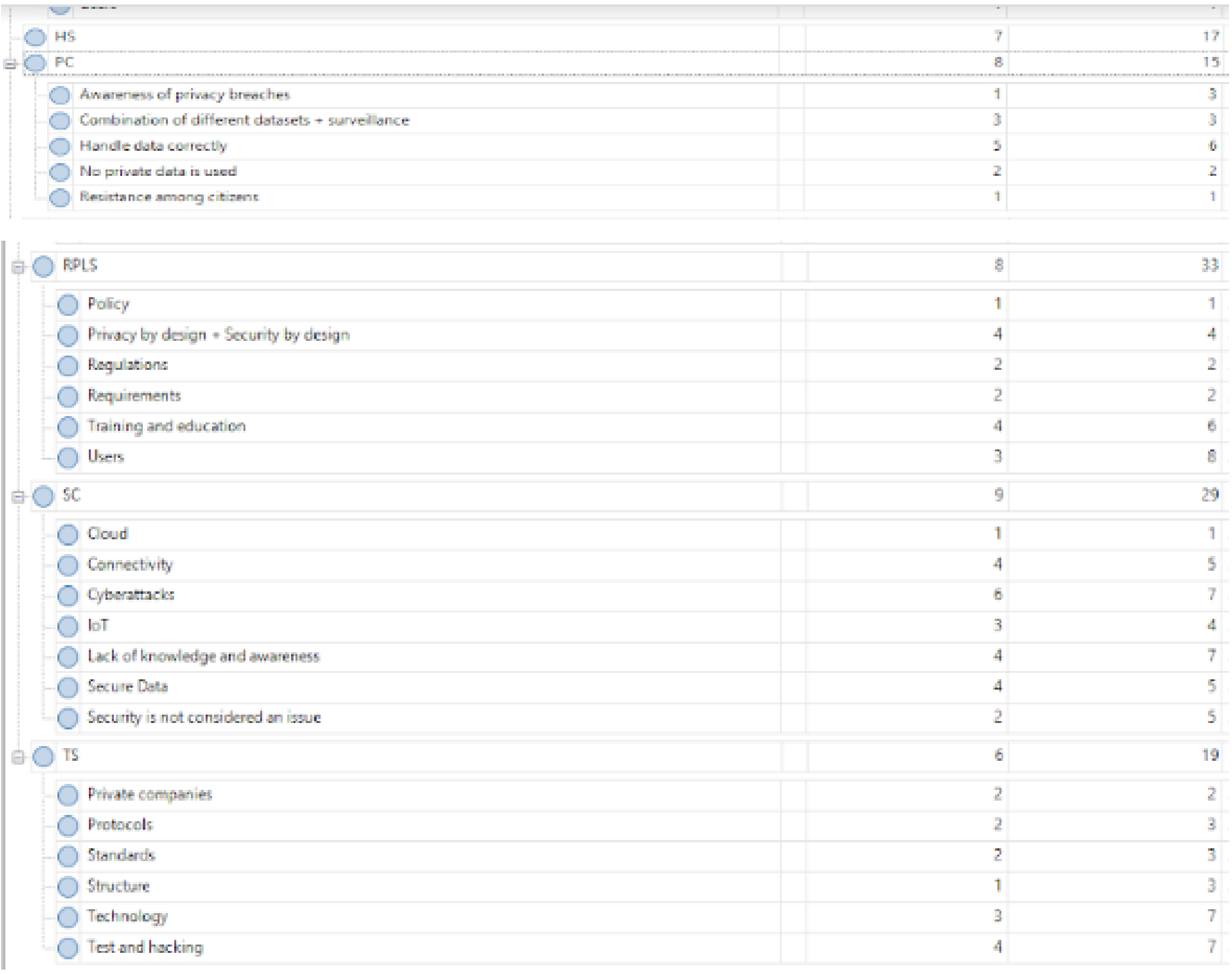
Base Nodes	Description of base nodes
PC	Privacy challenges
SC	Security challenges
CSP	Consequences of lack of security and privacy
TS	Technical solutions
RPLS	Regulatory, policy and legal solutions
GMS	Governance and management solutions
HS	Hardest solutions
FS	Future solutions

We also created sub nodes for the base nodes in NVivo since it made it easier to organize all our data. For instance, the base node SC (security challenges) had the sub nodes: 1) Cloud, 2) Connectivity, 3) Cyberattacks, 4) IoT, 5) Lack of knowledge and awareness, 6) Secure data, 7) Security is not considered an issue. To create sub nodes also helped us group higher-level categories to minimize the risk of having themes that are not uncovered (Recker, 2013). In Appendix 3 you can see an example of how we did the coding with base nodes.



Nodes

Name	Files	References
CSP	8	28
Loss of critical systems	5	7
Misuse of data	3	3
Physical harm	2	5
Problems with AI	1	2
Rate you as a citizen	1	1
Surveillance	4	9
Trust	4	6
FS	7	15
GMS	8	46
Board	1	1
Crisis management	2	6
Evaluate the systems	1	1
Experts	5	10
Information class	3	3
Objectives	3	3
Plan	4	5
Security mindset	3	3
Security project	2	2
Suppliers	5	5
Users	1	1
HS	7	17
PC	8	15
Awareness of privacy breaches	1	3
Combination of different datasets + surveillance	3	3
Handle data correctly	5	6
No private data is used	2	2
Resistance among citizens	1	1



HS	7	17
PC	8	15
Awareness of privacy breaches	1	3
Combination of different datasets + surveillance	3	3
Handle data correctly	5	6
No private data is used	2	2
Resistance among citizens	1	1
RPLS	8	33
Policy	1	1
Privacy by design + Security by design	4	4
Regulations	2	2
Requirements	2	2
Training and education	4	6
Users	3	8
SC	9	29
Cloud	1	1
Connectivity	4	5
Cyberattacks	6	7
IoT	3	4
Lack of knowledge and awareness	4	7
Secure Data	4	5
Security is not considered an issue	2	5
TS	6	19
Private companies	2	2
Protocols	2	3
Standards	2	3
Structure	1	3
Technology	3	7
Test and hacking	4	7

Figure 3.1: Coding summary from NVivo

3.7 Research quality

Research quality is reached through the conditions of reliability and validity. Reliability is described by Bhattacherjee (2012, p.56) as "the degree to which the measure of a construct is consistent or dependable". Validity, on the other hand, are described as "the extent to which a measure adequately represents the underlying construct that it is supposed to measure" (Bhattacherjee, 2012, p.58).

Achieving rigor in a qualitative approach is a bit different compared to a quantitative approach and other guidelines have been applied that are more suitable to the interpretive nature of qualitative methods (Recker, 2013). According to Recker (2013), dependability is achieved by demonstrating that measures provide similar results. To reach dependability, the interviews were transcribed by one researcher and cross-checked by the other. By doing this we removed possible errors in the transcript, and this resulted in higher reliability because of the higher truthfulness of the transcripts. When doing the coding in NVivo, higher dependability was also reached since we coded the sub nodes separately and these were later cross-checked by the other research partner to make sure that we came to the same results. In an empirical study, problems can arise about that the study contains subjective biases or poorly formulated questions and even if the questions are well formulated it is not sure that the measurement is reliable (Recker, 2013). To make sure that the measurement was reliable, the interview guide was constructed based on our literature review and the same interview guide was used in all interviews. We also made sure with the respondent that we share the same understanding of the concept Smart City.

Internal validity, also defined as credibility, concerns if the researchers have provided sufficient sustained evidence offered in qualitative data analysis (Recker, 2013). To reach high internal validity we have described clearly which respondents we have interviewed, how we have collected the data and what interview questions we have asked. We have also described how we have analysed the collected data with clear motivations of our methodological decisions as recommended by Bhattacherjee (2012). To make our study more credible, accurate records of interviews were retained and interviews were transcribed word by word. In the interviews conducted in Swedish we decided to provide the reader with both the Swedish transcription and the English transcription. Because according to Nikander (2008), hiding the original data from the reader's view violates the 'validity through transparency and access' principle.

Confirmability, also described as measurement validity, is a principles that postulates that qualitative research findings can be separately confirmed by outsiders in a position to verify the findings. To achieve confirmability, we send the transcriptions to the respondents a few days after the interview so they could confirm their statements.

External validity, also described as transferability, concerns whether and how much of the findings from a study can be generalised to other settings (Recker, 2013). To achieve high external validity, we interviewed respondents from three Smart City areas, instead of restricting us to one Smart City. We also interviewed at least two respondents from each Smart City area to get a more comprehensive finding of in what ways this Smart City area work with security and privacy. This will enable a high validity because if another scientific research is made based on the same scientific methods but instead targeting other Smart City areas, a similar result should hopefully appear. According to Recker (2013) very detailed descriptions of the research context should be provided, such that other can assess the extent to which the context characteristics match those of other fields of research. To reach this we provide a detailed description about our decisions for the research and for the interview guide.

3.8 Ethics

Research ethics is important because science has sometimes been manipulated in unethical ways by organizations and people to enhance their personal agenda and to be involved in activities that are opposite to the norms of scientific conduct (Bhattacherjee, 2012). With information systems research being a social science, an ethical principle in research conduct is the need to be knowledgeable of having the responsibility to secure the real consent and interests of all those involved in the study (Recker, 2013). The researcher has a responsibility to protect the rights of people in the study as well as their privacy and sensitivity (Recker, 2013). This was something we had in mind during the whole research process.

In qualitative interviews it is important to obtain the subject's consent to participate in the research, voluntary participation, to secure their anonymity and confidentiality, to inform them about the character of the research and about potential risks and also inform them about their right to withdraw at any time (Brinkmann & Kvale, 2005). To achieve this, we first of all sent them an email about the character and purpose of the research and they had the right to withdraw if they did not want to participate. Before the interview, we asked them if they wanted to be anonymous to achieve the anonymity aspect that Brinkmann & Kvale (2005) mention. Even if no one wanted to be anonymous we choose to not use their names in the research to protect their anonymity and confidentiality. It could still be possible to assume who the respondents are because we provide their job title. However, because it was okay for everyone of the respondents to present their name, that is not a problem. When the transcriptions were done, we sent them to the respondents so they would feel comfortable with their answers and otherwise they had the possibility to change their statements.

We preferred to have the interviews in English to not interpret the data in the wrong way. Because when we translate from Swedish to English the result might not be the same as the respondent intended it to be. In the cases when the respondent preferred to have the interview in Swedish, we agreed with that but then we translated the transcription from Swedish to English to make the process of coding and analysing easier. Both researchers also checked the transcript, so the translation was not perceived in a different way than the original transcription. We provide the full transcript of the Swedish transcription in appendices but also the translation in English.

When doing data analysis we took into account that we completely reported how our data was analysed, for instance we provided the full transcripts in the appendix, we described how we transcribed and coded the data and what tools we used, which is in accordance with what Bhattacherjee (2012) write about ethics regarding analysis and reporting. We also include quotes in the empirical results and discussion.

4 Empirical results

This chapter describes the analysis of results which were acquired following the methodology applied in the previous chapter. The chapter presents the result in a synthesized manner pointing on commonalities and differences in what the respondents said. This section is structured like our research model and includes subheadings of the key concepts identified.

4.1 Security challenges in the Smart City

All the respondents mentioned security as a challenge except for R5 who thought that people are more focused on development and innovation of new solutions and to get them out on the market (Appendix 6: 70). This is in line with what one expert mentioned on the focus-group interview. E2 mentioned that vendors often develop tools without thinking of neither security or privacy, they just want the product to be out there which leads to that people can expose these devices (Appendix 1: 31). One security challenge that was discussed by one expert that was not mentioned among our respondents was the cloud as a security challenge. E1 pointed on that the cloud can be very risky since you do not know what is happening inside or behind the cloud (Appendix 1: 53).

So, the cloud while they help in a way that reducing the cost of the devices because you don't need to have onboard storage and processing and sophisticated software onside the device. It is at the stake of user privacy. So, what is happening inside these clouds. So that is one thing, cloud might be very risky in a way. (Appendix 1:53)

4.1.1 Connectivity

Connectivity is a security challenge brought up among some of the respondents (R2 and R3). The challenge can be in Smart Cities when you put many puzzle-pieces together, it can create holes in the whole puzzle that can offer opportunities for someone to break in (Appendix 3: 26). R3 explained that it exists security protocols so you can secure one A to B technology but when you change from the gateway to internet protocol, the gateway can open the data and then attack the new way (Appendix 4: 6). But this is something they want to tie so they have higher security.

[...] when you put many puzzle-pieces together it could build kind of holes in that whole puzzle that could offer opportunities for someone to break in. (Appendix 3: 26)

R4 also recognized a security challenge related to connectivity, but R4 described it as when more and more things are being connected to the internet it results in that the ability to attack increases (Appendix 5: 32).

4.1.2 Internet of Things

Security challenges related to IoT are recognized among two of our respondents and one expert (E1, R3 and R7). E1 described that with Internet of Things we have stepped more back than before when it comes to security among devices because they seem to be more open (Appendix 1: 86). E1 also pointed out that Smart Cities will use IoT and the security will often be insufficient first but later on some might start think about it (Appendix 1: 86). R7 are involved in a Smart City project that is in the elderly care area and R7 pointed out that in elderly care it is security risks already but with the implementation of IoT in the project it is a higher risk of devices being hacked or compromised (Appendix

8: 16). R3 mentioned that security is not added to the IoT devices and that is what makes it the most vulnerable place regarding security (Appendix 4: 34).

Because in normal cases today, the most vulnerable place is the IoT device because people are not adding the security [...]. (Appendix 4: 34)

4.1.3 Secure data

To have secure data and information so it is not misused is something that R8, R1, R4 and R7 discussed. R8 mentioned that it is of importance to have infrastructure security so you cannot hack into the data or misuse it, it does not need to be personal data involved (Appendix 9: 20). You can change blockage in the city, water or utility, or misuse data in some way that is not thought of yet (Appendix 9: 20). To make sure that you can trust the data is important (Appendix 4: 18). To have secure and anonymized information is crucial according to R1 due to all the data they have about the citizens (Appendix 2: 28). R1 pointed out that some information is not necessary to have such high detail on (Appendix 2: 28). R7 also mentioned that it can be consequences if you get physical access to the infrastructure and get the data that runs through the gateway like this (Appendix 8: 22).

We have seen that there are all the time challenges when it comes to security from different ways. For the first, it must be secure information because all the data we have about our citizens. (Appendix 2: 28)

4.1.4 Cyberattacks

Among our respondents there is no one who mentioned that there have been any cyberattacks against their city. They either answered no on this question or they said that they have not had any knowledge of that it has been a cyberattack. Although, R8 said they have not had any incidents that they know of, but they have, for instance, sensors and gateways which they have thought being not secure enough (Appendix 9: 34). R4 pointed out that there are projects that are still mostly pilot which can be a reason for them to not have received any cyberattacks (Appendix 5: 42). R6 said that they have not been affected in the municipality that they can say from cyberattacks but R6 is the only respondent that mentioned that they have had one attempt to infringe, but it did not result in any bigger issue (Appendix 7: 14).

We have not been affected in the municipality as we can say. People have certainly been trying or I know we had one attempt to infringe, but it has not become any greater of the least that has hit the business. (Appendix 7: 14)

4.1.5 Lack of knowledge and awareness

Security challenges that are related to users are discussed by three respondents (R6, R7 & R8) and two experts. E2 mentioned that where there are humans there is a lot of security risks (Appendix 1: 60). It can be challenges relating to update the security of the devices since a device that is used throughout the years will need to be updated/upgraded and how does the user update the security. E2 pointed on the question of how companies or vendors send notification to the users about that they need to update because they might have a new security aspect on this device. Security mechanisms evolve and hackers constantly try to access these devices (Appendix 1: 43). E1 also mentioned that users can range from very technical to not technical at all which leads to that for some users it might not be difficult to upgrade a software but harder for other users. It is needed to take into account that you are not always working with highly technical people (Appendix 1: 42).

R7 mentioned that one of the greatest challenges related to security is that some employees are not very used to technologies and they might not have the right education or language skills which can result in security risks (Appendix 8: 26). R8 pointed on that employees need to have a lot of insights about the security challenges, but this is not always the case and employees are not 100% knowledgeable about security challenges (Appendix 9: 24). The lack of knowledge is a security challenge according to R8 (Appendix 9: 24).

[...] of course, the employees know that you need to have a lot of insight about this, but they don't necessarily know, they are not 100% knowledgeable about security issues and all Smart City solutions so we always ally ourselves with experts within our own organisation but sometimes also externally. (Appendix 9: 24)

E1 said that it is a big problem when not technical users can access available tools with very great ease, for instance accessing cameras that use default passwords and with a click on a button you can get all types of information (Appendix 1: 25).

4.1.6 Security is not considered an issue

Vendors that develop different tools do not think about security or privacy according to E2 since they most often just want the product to be out there. This leads to that these tools can lack appropriate security mechanisms (Appendix 1: 31). E2 mentioned that it is most often small companies that do not think about security and privacy, they do not think about it from the beginning and they might start think about it later on but then the product is already out (Appendix 1: 35). R5 was not considering security as a challenge in their organization since it is nothing that is brought up that R5 knows of and this could be due to a lack of competence (Appendix 6: 50). R5 also pointed on that most people want to innovate and come up with a new solution and implement it on the market and that might be a reason to why they do not have security as their focus (Appendix 6: 70).

Because it is very technical, it is driven from technical, from needs of technical solutions water management problem or waste management problem and security is nothing that is brought up, it could be due to lack of competence maybe. There is not an issue that people bring out. (Appendix 6: 50)

4.2 Privacy challenges in the Smart City

Most of the respondents recognized security challenges and that challenges related to privacy was more of a consequence due to the lack of security and consequences that are presented under paragraph 4.3. Although, some challenges that are more related to privacy was discussed during the interviews.

R1 said that a challenge related to privacy can be when two or three data sources can be combined and tell something they did not even imagine was possible, a challenge that is about combination of different data sources (Appendix 2: 39). R1 also mentioned that this is something they talk a lot about. R3 mentioned that when you have a lot of information in the city it can be possible to track people with cross-coupled information and that is something hard to prevent (Appendix 4: 18). Privacy challenges in terms of use of cameras, GPS, information that is linked to people’s behavior and how they move in the city are mentioned by R5 (Appendix 6: 28).

But one thing that crossed my mind, one and a half year ago in the beginning of the smart and public environments 2 is that when you have a lot of information in the city you could actually be able to *track people with cross coupled information and that is something that is very hard to prevent.*(Appendix 4: 18)

To be aware of when you are breaching the privacy is something that R8 discussed as a challenge (Appendix 9: 38). Some privacy challenge is regulated by law and are beyond the GDPR and other times the GDPR applies. R8 really pointed on that it is important to know when you are going to far and breaching privacy (Appendix 9: 38). The respondents are aware that some data can be a piece of privacy data, for instance data that they use might not be private from the beginning, but it can become private together with other data. Some respondents said that they don't use private data so privacy might not be a challenge. R2 for instance said that they do not use that type of data, but they realize that it is possible to maybe dig back and connect some sort of data to see who is doing what. But they try to make sure that the data is not connected to a person in their projects (Appendix 3: 30).

I think the biggest challenge is, yeah that is a good question. I think it is being aware of it when you actual breaching it, when you are going to far. (Appendix 9: 38)

According to R1, when privacy is breached it can lead to that people become skeptical and that people do not dare to be public and honest which is a big problem (Appendix 2: 47).

4.3 Consequences of security and privacy challenges

The consequences the respondents mentioned as a result of inappropriate security and privacy solutions are presented under this section.

4.3.1 Loss of critical systems

A consequence that was mentioned among one expert (E1) and four respondents (R4, R5, R6 & R7) was loss of critical systems, and with critical systems it is meant systems that makes the city work. E1 said that for instance with smart energy you can black out the whole city if you take down the electricity (Appendix 1: 20). Consequences related to if the electricity goes down is related to something that R7 also discuss, loss of internet connectivity would have bad effects for the city and citizens (Appendix 8: 26).

Because you might affect the electricity of a country. You can for example have a text that black out the whole city for instance. (Appendix 1: 20)

If you could set out solutions which makes the region loss the mobility could have bad consequences for the transport according to R4 (Appendix 5: 52). R4 mentioned that shot out of the electricity could have consequences for the city (Appendix 5: 54). R5 stated that energy and water are vital infrastructure for the society and for the cities so it could be an issue if you lose this in the city (Appendix 6: 38). According to R6 the city is extremely sensitive and if we get rid of something for a long time, like internet, it means we can not go shopping and get our money out, for instance (Appendix 7: 32).

And the energy system. If you could shut-out the electricity of things. So, I think that you have some major critical areas which you could basically close down and maybe more or less a whole society. (Appendix 5: 54)

4.3.2 Datafication

Surveillance as a consequence of security and privacy challenges are recognized among all experts (E1, E2 & E3). E2 mentioned that on a study on cameras they could access thousands of cameras and on these they could see people living, taking baths and kids playing (Appendix 1: 26). It would also be possible to install a camera in a nuclear power plant to view on what is going on, according to E3 (Appendix 1: 41). And if you can hack these smart systems you can see when someone entered the metro and also when going off, and this could be a problem especially if you are a political figure, E3 mentioned (Appendix 1: 74). E1 described that in Smart Cities we are becoming like a society that are being surveillance all the time and E1 also pointed on if you are having a free choice if someone is always monitoring you (Appendix 1: 62).

Because in Smart Cities we are becoming like surveillance, like a society being survey all the time and this is a big topic. Do you have free choice if someone is always monitoring your daily lives, your daily habits. (Appendix 1: 62)

This consequence is also mentioned by some respondents (R7 & R3). R3 described that you can track people and find where they are working, where they shop groceries, where they live and which kindergarten they leave their kids at (Appendix 4: 20). You can track patterns for each individual and you can use this data for commercial purpose if you have access to this data (Appendix 4: 20). According to R7, it becomes possible to measure, watch every step people make and collect data about blood pressure for instance (Appendix 4: 24).

If that data comes out and you can find this on the net you could start track and find where people are working, where they shop their groceries, where they live, which kindergarten they leave their kids at. Then the people can track exactly the pattern for each individual person and then suddenly you get different angles how you use that data for commercial purpose, and so on and then they will nag that person in the end with advertisement and that is not nice. (Appendix 4: 20)

In this type of society, it can be possible to score how someone behaves online, it can be possible to be scored as a good or bad citizen based on data that comes from when tracking someone, according to E3 (Appendix 1: 91).

4.3.3 Loss of trust

Four of the respondents (R2, R7, R4 & R8) mentioned lack of trust from citizens as a consequence if a cyber attack or privacy breach would happen. R2 said that if something happens you do not have trust in the system and the data that comes out of it, which can lead to that the system becomes useless (Appendix 3: 22). It can also become harder to run some sort of Smart City projects if you do not have user trust (Appendix 3: 34). R8 pointed on that people will be against implementing more Smart City solutions if something happens (Appendix 9: 46).

Hesitancy to accepting these kind of technologies in the city can be a consequence according to R7 therefore they point on that they are very careful in their organization (Appendix 8: 20). R4 said that trust can be gone as a consequence if something happens. It is like a friendship and it takes long time to build trust but only short time to destroy it (Appendix 5: 62). If it is destroyed it will also take large amount of resources and initiatives to build it up again.

I would think that our end-users or customers would be more hesitant to accepting this kind of technology in the care and of course also for us in the city it would mean that we would be […]. (Appendix 8: 20)

4.3.4 Misuse of data and physical harm

Misuse data to do bad things to the city is recognized among three respondents (R2, R8 & R3). R8 mentioned that you can do "evil" things if you misuse or hack the systems or to benefit your own purposes (Appendix 9: 44). To change information and control things in different ways can be a consequence according to R3 (Appendix 4: 32). It can also be possible to, for instance, send out a lot of emails if sensors are hacked but R3 pointed on that if only one sensor is hacked a lot of damaged might not happen. R2 described that if you tample with data you can probably make a lot of damage, especially if the data controls something else, like a whole system or something else that is important (Appendix 3: 22).

The experts (E1, E2 & E3) brought up physical harm as a consequence of lack of security. For instance, if you have a health issue and do not want to expose yourself or if you are dependent on an IoT device that keeps your life going, like a pacemaker (Appendix 1: 31). E2 said that it might be common nowadays that someone might hack that device if there is lack of security (Appendix 1: 31). Imagine if someone has assisted living and medication at home, and the data is changed that the person sends to the healthcare provider, that could lead to bad consequences, like death, according to E1(Appendix 1: 62). R4 also pointed on that it can have consequences like people getting wrong treatment or medicine and it can be a matter of life and death (Appendix 5: 52).

Well, of course health is a challenge because it could be a matter of life and death. People getting wrong medicine and so on, or wrong treatment or whatever. (Appendix 5: 52)

E1 said that in car services, if someone hacks the system, it can be possible to change the speed of the car or break the distance automatically (Appendix 1: 62). E3 mentioned that it can be possible in a future Smart City to hack the AI that controls self-driving cars and what can be the consequences of that? It can be more severe consequences if it is a malicious attack towards all cars on the road if they create an entire system (Appendix 1: 55).

4.4 Solutions to security and privacy challenges

In what ways the Smart Cities work with security and privacy challenges according to the respondents is presented in this section.

4.4.1 Technology solutions

Best practice solutions

Both R2 and R3 described that they use standard security protocols in their projects. R3 described that protocols will be used in a real environment to go through all different kind of technologies and this has to be done before (Appendix 4:8). R3 continued to describe that they use standard components from the industry, real stuff that you can buy from the market R3 described (Appendix 4:8). R2 also discussed that when it comes to the cloud platforms and those things, they try to use industry standards to build up the systems (Appendix 3: 40). No more respondent mentioned that they use protocols or standards.

One important part, according to R2 and R7, is to have a good architecture when they create the Smart City environments. According to R2, Lund is at the moment trying to build a reference architecture of what kind of security measures that are needed when they implement projects in the city in the future (Appendix 3: 26). R7 also mentioned that it is important to have good information models and follow that in the architecture when they build the IoT and Big Data environments (Appendix 8: 32).

And that project, they are running it as we speak so it is not finished. So, basically what the outcome we hope with that project is that they give us kind of a reference architecture of what kind of security measures we have to take when we build up this kind of metrics. (Appendix 3: 26)

R7 also mentioned that they need to develop or build a good information structure, so they know exactly where they have which data (Appendix 8: 76). R4 also described in line with this that the data infrastructure is important and the collection of data, data sharing and how to handle the data (Appendix 5: 10).

All of the cities try to secure the technology in the city in some way. When it comes to make sure that the technology in the Smart City is secure, R1 described that they will probably work in some ways to make the technology secure in the city when the technology is implemented (Appendix 2: 63). However, R1 do not know if that solution will be enough. R1 also described that they work a lot with reducing the number of people that have the right to enter their systems (Appendix 2: 63). This is something that also Lund will start work with to see what kind of people that have access to their systems according to R6 (Appendix 7: 50). R7 described that for their data connectivity they already work with data connectivity. They also work with firewalls on their servers and data encryption when they send something over the internet (Appendix 8: 38).

Well of course for our data connectivity we work with firewalls already. And anything that is on a server we also work with firewalls and also data encryption when we send something over the internet. When we precure solutions that are cloud based or such we put in our requirements, we have security requirements. And then I would also say that, I mean a part of the purpose of this Vinnova project we are doing is to develop better security for IoT devices and to develop a standard. (Appendix 8: 38)

R8 described that they try to protect their sensors in the street with the hardware. They also think about how they do the setup, how they do protection and hardware protection (Appendix 9: 54). They also have malware protection and firewalls and things like that. They also have people watching over the data packages (Appendix 9: 54).

R3 described that they started a security project with RISE, Sensative and U-blox to make sure that the data from the sensors to the cloud is completely secure (Appendix 4: 6). They started an objects security system, so the object is secure so even if the object goes between different technologies the information is never revealed. The information will not be tackled, and no one will be able to reach it without the encryption keys (Appendix 4: 6). R3 also described that they work with filtering the data so no one will be able to see the start and stop to make sure that no sensitive data will be revealed (Appendix 4: 20). Furthermore, R3 described that they evaluate and certify the sensors in different levels depending on what security level they would like to have on these (Appendix 4: 38). R3 gave the example that if there is a simple sensor for measuring the temperature it is not very sensitive data and it does not need to be very reliable and no one is interested in this kind of data either. Those kind of sensors could therefore be easy certified (Appendix 4: 38). R6 described that they have both firewalls and warning systems so they can shut down if it is necessary (Appendix 7:16). They also have the robustness, they have two servers and data is added on the server every night so there is back-up all the time, one of the servers even have cloud service as well so the back-up is always there according to R6 (Appendix 7:16, 46).

Mobile heights together with RISE and Sensative and also U-blox started up a discussion how do we secure the sensor that to make sure that the data come from the sensors to the cloud that it is completely secure. (Appendix 4: 6)

Security testing and Smart City cybersecurity lab
Testing is something that all the cities work with. R7 mentioned that they do security tests and R1 mentioned in addition to this that when they have the technologies implemented in the Smart City, they will start test their smart applications (Appendix 8:40; Appendix 2: 20). R2 described that they have a testbed but this one is not specialised on security, instead they have a project on the side that is totally focused on security, and this project is not run by the municipality (Appendix 3: 18). The project is run by mobile Heights and RISE and RISE have a security lab in Lund. So, they are testing the things they build up and the testbed is a ground to see how safe it is and what kind of measures they need to take to make sure that they have a secure system. R3 also described that they collaborate with RISE which have been testing the products in the labs (Appendix 4: 10).

R4 from Copenhagen described that they have established a Smart City cybersecurity lab at the technical university where they work on the high security and privacy challenges (Appendix 5: 32). R4 continued to describe that they have recently launched a hackathon and when they do projects, they will try to link these to this Smart City cybersecurity lab, and they will do some testing there (Appendix 5: 32). R4 mentioned that in many solutions the companies are responsible for the IT security but on the hackathon, they try to make a better link to companies (Appendix 5: 34). R8 also mentioned that they have a collaboration with the university and that they have a hack lab that they use to try to fix some of the issues they think that they might have (Appendix 9: 34). R8 also described that security wise they test the data, so they have the right setup, but they do not have a specific test environment for this (Appendix 9: 84). R8 described that they do not have a living lab or a test lab, but they can test in the Skylab if they need that. R8 further describe that they do a lot of live testing in the city but then they do it as a part of a pilot project or a proof concept (Appendix 9: 89).

In addition to the testing and hacking R3 mentioned that today it is extremely uncritical data that they handle in their systems (Appendix 4: 28). Therefore, it would be quite funny if someone would try to hack the system because then they can learn R3 described. They can learn how they do and what they need to do if they try to hack it, according to R3 (Appendix 4: 28).

Something that both R8 and R3 mentioned is that there is not one solution that is the most important one, instead all the solutions are together important to make the Smart City secure. R3 described that if someone gets in anywhere in the system, you will open up the full systems so you cannot say that one thing is more important than another. Because if the attacker finds a hole to go into it does not matter where it is (Appendix 4: 48). R8 described that all solutions together are important:

I would say that all together is important not one alone. I think that is very important, you can never look at things isolated always, if you implement some kind of system then you also suppose, you have to see it in collaboration. One does not go alone. (Appendix 9: 58)

4.4.2 Policy, regulatory and legal solutions

When the Smart Cities purchase and implement technologies from different vendors, they have some policies, regulations and requirements on the vendors but there are also regulations that the Smart City need to follow according to the respondents. R8 stated that when they precure solutions that are cloud based or such they have security requirements and they have multiple requirements on their IT vendors (Appendix 8: 38). R1 mentioned in addition to this that when they start with their new projects, they start with identifying what aspects they see as general for all projects and they need to formulate regulations that should be for the entire city (Appendix 2: 59). It can also be policies about how you should do to be allowed to implement a sensor and share the information according to R1 (Appendix 2: 59).

R8 mentioned that there are some rules they need to follow, one example is GDPR that they are fully applied to or at least try to be fully applied to (Appendix 9: 50). R4 mentioned in line with this that there is some guidance on the national level they need to follow (Appendix 5: 50). For example, the GDPR and some things, things you need to implement in every institutions according to R4 (Appendix 5: 50). R3 mentioned that the companies that work in their projects need to work with security and privacy because that is basically the law more or less (Appendix 4: 42). In addition to this R6 made a point that even if they have all these agreements between the municipality and many different vendors, if anything happens, they cannot do anything anyway, even if something is written in the contract (Appendix 7: 40). E2 also stated that especially small companies they never follow these legal aspects (Appendix 1: 101).

It is also hard to follow legal aspects, especially small companies. They never follow these legal aspects. (Appendix 1: 101)

Two of the respondents, both representatives from Lund, mentioned that they have regulations and policies for the citizens or the users of the Smart City. R2 described that they try to have policies or agreements towards the users in the Smart City (Appendix 3: 36). In addition to this R3 described that in the project of tracking bikes and how they show this information, each individual person has written that it is okay for the company to get this information, agreements with the users (Appendix 4: 20).

Privacy and Security by Design

Privacy and security by design is something that is used in all the cities. R8 described that first of all they identify if they need private data in the project and how they can minimize the access of private data (Appendix 9: 70). R4, also from the same Smart City area as R8, said that they have tried to work more or less with privacy and security from the beginning (Appendix 5: 32). In addition to this R4 mentioned that the idea is to link projects to the Smart City cybersecurity lab that use to work with privacy and hacking security private line (Appendix 5: 78). R7 from Stockholm stated that they work with privacy by design and security by design since they have it in their IT architecture and in their requirements and it is something they consider every time they purchase or develop something together with their partners (Appendix 8: 42). R3 from Lund mentioned that they do not, from a project view, look into design for privacy and security, but that the private companies within these projects need to work with that (Appendix 4: 42).

[…] we have been trying to more or less build in privacy and security from the beginning. (Appendix 5: 32)

Education and training

There are mixed responses from the respondents about education and training. R2 from Lund mentioned that they have not had any training or education when it comes to security, but they have had training for how to use networks, how to connect sensors and build it up (Appendix 3: 62). R6 from Lund municipality mentioned that they have one person at the IT-department that work with employee training (Appendix 7: 20). R4 from Copenhagen mentioned that they had education where they tried to do the citizens' more competent and skillful in handling different kind of pass and compute Smart City solutions (Appendix 5: 82). R8 also from Copenhagen mentioned that they have projects where R8 dialogue with the colleagues or with the citizens about Smart City challenges (Appendix 9: 26). R7 from Stockholm described that they are planning and will very soon have a general information security training for everyone that is new in the organization (Appendix 8: 44).

Yes, we do but we haven't done it when it comes to security in that sense. But we have been working with, we have had training for instance how to use the different kind of networks, and how to connect sensors, how to build it up. (Appendix 3: 62)

4.4.3 Governance and management solutions

Leadership and planning
Four respondents (R1, R2, R4 & R8), representative from all of the three Smart City areas stated that they need to have a plan and they need to identify what the risks can be before they start with a Smart City project. R2 mentioned that if you want to do those type of projects you will have to plan before you go out (Appendix 3: 34) and R4 mentioned that in the projects they work with they have tried to work with privacy and security from the beginning (Appendix 5: 32). R8 mentioned that before they start with the projects, they go through what kind of known risks there are, and especially when personal data is used in the project (Appendix 9: 66). R1 stated that they always need to bring in security questions to the projects that are performed, and they have to think about what the risks can be from different aspects. R1 also mentioned that they can not leave the security questions to an expert and instead they need to work together with the experts to be able to work with the security and privacy in a good way (Appendix 2: 51). R1 also stated that it is important that everyone in their projects need to think about the security and privacy questions all the time (Appendix 2: 67).

Yes, the most important is that we always have it in mind from all aspect. I think it is important that everyone that work in our projects thinks about these questions all the time and then that we collaborate with experts and ethical questions that are important. (Appendix 2: 67)

Objectives
Objectives for security and privacy is nothing that is defined in the Smart City according to the respondents. Respondents from each of the three cities responded that they do not have any objectives when it comes to security. R2 mentioned that they have not had focus on security in their projects, so they are not setting any goals (Appendix 3: 40). R8 said that they do not have any defined goals for security. It is a goals in itself to secure R8 described (Appendix 9: 74). R5 stated that they do not have any goals for security because security is not an issue (Appendix 6: 48). R1 also mentioned that they do not have any goals when it comes to security, it is something obvious (Appendix 2: 57). In contrast to this R7 thinks that they have goals for security but when R7 described this further it was more about an overall information security policy (Appendix 8: 62).

No, we don't. This is a goal in itself to secure that but that is the data is secure but also that we have secure seat of data is also an issue. But nothing more specific than that no. (Appendix 9: 74)

Vendors and evaluation
Something that was identified in the interviews were that much of the responsibility for security and privacy is on the vendors of the technologies in the Smart City. R4 mentioned that in many solutions are the companies responsible for the IT security (Appendix 5: 36). R8 agreed with this and mentioned that the utility companies are responsible for the security in the Smart City (Appendix 9: 60). R5 said that there are the energy companies that are responsible for the water management systems of the energy systems and is therefore also responsible for the security in these systems (Appendix 6: 44). In addition to that much of the responsibility is on the vendors of the technology in the Smart City, R2 mentioned that they push a lot of responsibility towards the end-users (Appendix 3: 36). R2 said that when the users use the network the users have to make sure that they do not break any laws or do anything that they are not allowed to do (Appendix 3: 36).

But in many solutions, the companies are, are responsible for the IT security […]. (Appendix 5: 36)

Two of the respondents (R1 & R8) mentioned that they work with evaluation of the technologies from the vendors. R1 mentioned that they have a security company involved when they purchase technologies and this company go through the purchases to make sure that they have thought as far as they can (Appendix 2: 65). R8 also mentioned that they evaluate the technology they implement (Appendix 9: 103).

Experts and security/privacy team
Five of the respondents (R1, R2, R3, R4 & R7) representative from all the cities said that they work with experts within security. R2 said that because they do not have the knowledge about security in the municipality, they have a project together with Mobile Heights, RISE, Sensative and U-blox and these companies try the things that Future by Lund develop. They test how safe the technology is and what kind of measure they need to have to make a secure system (Appendix 3: 18). This is something that also R3 mentioned, that Mobile Heights, RISE, Sensative and U-blox started a discussion about how to secure the sensors (Appendix 4: 6). Stockholm also use experts to make sure that the Smart City is secure according to R1 and R7. R1 stated that it is important that they collaborate with experts (Appendix 2: 67) and R1 said that they have employed a company that will help them do the right things when it comes to security-questions and this company works with the security all the time (Appendix 2: 30). R7 also mentioned that they have people that are responsible for the information security and these people work daily with the security challenges (Appendix 8: 60). Even Copenhagen have experts that they work closely with according to R4 (Appendix 5: 89). When they start new projects, they collaborate with the Smart City cybersecurity lab (Appendix 5: 93). R8 also mentioned that the utility companies are responsible for the security in the Smart City (Appendix 9: 60).

Yes, the most important is that we always have it in mind from all aspect. I think it is important that everyone that work in our projects thinks about these questions all the time and then that we collaborate with experts and ethical questions that are important. We have that in mind all the time, that is important. (Appendix 2: 67)

City emergency response team
All the cities have a team, responsible for the security in the city if an emergency happens. R7 from Stockholm mentioned that they both have procedures together with their IT partners and then if something bigger happens, they have crisis management in the city (Appendix 8: 56). This is in line with what R6 from Lund mentioned. They have a crisis preparedness, a whole staff that can get started, a crisis management staff (Appendix 7: 62). R6 mentioned that they are prepared and that they have a plan if something would happen (Appendix 7: 84). R6 stated that it is important that they have redundancy and back-up of important functions in the city and that is something they work with (Appendix 7: 40). R8 from Copenhagen mentioned that the utility companies in the city are responsible for the security in the city and they have 24 hours of surveillance (Appendix 9: 60,62).

Yes, so... we have a crisis preparedness, a whole staff that we can get started, a crisis management staff. (Appendix 7: 62)

Privacy and security board
Just one of the respondents mentioned that they have a board related to security and privacy. R4 stated that Copenhagen has a board where they discuss different kind of problems related to privacy before they roll-out a digital solution in the city (Appendix 5: 50).

4.4.4 Hardest solutions

The respondents had some mixed opinions about what solutions that are the hardest and takes the most time and resources. R7 mentioned that the solutions that takes the most time and resources is to educate people because there are a lot of people to educate (Appendix 8: 72). R7 described that users do not know how to use the technology and then it does not matter what other kind of security you have (Appendix 8: 66). R6 mentioned something in line with this. According to R6 is it hard to create an awareness among the employees and the citizens about security and that is what R6 believe they work the most with (Appendix 7: 66). R8 also mentioned that one of the biggest challenges for the security in the Smart City is the lack of knowledge of the security (Appendix 9: 22).

According to R3, one of the hardest challenges with security solutions are that security of a system is never ended:

You have to continuously work with the security because new things show up and people are finding new ways of hack it and so on and you need to keep them updated. (Appendix 4: 36)

You need to have the security all the way down to the sensors. If these updates are not done you will be hacked sooner or later, R3 described (Appendix 4: 36). R3 also mentioned that the things that take the most time is to test it, there is never an end for testing (Appendix 4: 50). In accordance to what R3 mentioned, R1 mentioned that security is nothing they can say that they do not have any more money for security, instead R1 explain that they must all the time be able to develop their services with the highest security (Appendix 2: 69).

R8 mentioned that the solutions that take the most time and resources for them right now are working with the data in camera technology. The camera technology is something that is new for them and they need to understand and figure out how to use it in the right way (Appendix 9: 76). Furthermore, R8 explained that the camera technology takes long time because they have a lot of personal data and they try to eliminate as much of the personal data as possible (Appendix 9: 78).

Because there can be a breach and if it is a number of camera feed of pictures there would be able to identify persons and that is something that we are designing data for not trying to do so we are thinking very much about in edge computing and trying to eliminate as much of personal data as possible so we just get the feed of counting of people and not necessary who it is. (Appendix 9: 78)

According to R6 one of the things that take the most time is all the preparatory work and planning and what to do to be as safe as possible if something happens in the city. Further R6 mentioned that they do not have so much resources for security when they are in the planning stage (Appendix 7: 70).

4.4.5 Future solutions

A variety of perspectives were expressed from the respondents about how they will work with the security and privacy in the Smart City in the future. R1 from Stockholm mentioned that they need to see what happens on the market and see what the risks are because there might always come new risks that they have not thought of and that is their big challenge (Appendix 2: 71).

It is important to have jour with the rest of the world and understand what happen and have a view on the rest of the world all the time. (Appendix 2: 73)

R7 cannot, in contrast to R1, think of anything of how they will handle the security and privacy challenges in the future (Appendix 8: 78). R4 suggested that they need to cooperate with researchers or private companies and experts in the field. They also need more or less try to work together with the public sector, the private sector and researchers R4 described (Appendix 5: 89).

On the other hand, R6 described that in Lund they have made a new security program that will apply throughout the municipality (Appendix 7: 76). Lund are also hiring more people that will look at the security and privacy challenges, R6 mentioned. Furthermore, R6 mentioned that in the future they will collaborate more between Future by Lund and Lund municipality. In addition to this, R2 hope that they will get a large part of an architecture of how the security solution should be implemented over the whole system. R2 described that they want this so they can implement this solution on the test-bed afterwards to make sure that they have a fully complete system from the end-sensors all the way through the systems to the cloud network (Appendix 3: 56).

R3 have an idea that AI can be used in the Smart City as a system that can learn that when new sensitive data is added the system can learn how you track people. R3 thinks AI is the next step because you can not have people for that, sit and analyse the data, and if the data is not analysed and if no one have made sure that the data is correct then the system will be unreliable and that will no one like to use (Appendix 4: 18 & 52). Despite R3 no one of the other respondents mentioned AI as a solution.

4.5 Summary of empirical results

4.5.1 Concept 1: Security challenges in the Smart City

Overall, the results indicate that the respondents see security challenges related to connectivity, IoT and secure data. On the contrary, cyberattacks and security is not considered an issue was two aspects that was not brought up by the respondents. Respondents brought up consequences related to cyberattacks but not anyone had received a cyberattack that they know of. It was only one respondent who mentioned that security is not considered an issue in their organization. Lack of knowledge and awareness was considered an issue both among respondents and two experts.

4.5.2 Concept 2: Privacy challenges

The respondents mostly recognized challenges related to privacy concerns was more of a consequence due to the lack of security. Although, privacy challenges that was brought up by respondents were about combination of different data sources so you can track people, to be aware of when you are breaching privacy and going to far and that data which is not considered private from the beginning can become private together with other data

4.5.3 Concept 3: Consequences of security and privacy challenges

Consequences of security and privacy challenges that was mentioned by the respondents were loss of critical systems, datafication, loss of trust and misuse of data. Loss of critical systems and loss of trust was two aspects that was mentioned by four respondents on each aspect. Loss of critical infrastructure was also brought up by one expert. Datafication was discussed by all experts and by two respondents. Misuse of data was a consequence that was mentioned by three respondents. Physical harm was a consequence that was brought up by only one respondent, but it was mentioned by all experts.

4.5.4 Concept 4: Solutions to security and privacy challenges

The result imply that technical solutions are used in all the Smart Cities, but they are used in some different ways. The factors identified from all the interviews are firewalls, encryption, architecture, standard components and information access. The result also indicate that security testing is used in all the Smart Cities before the technology is implemented in full-scale in the Smart City. One of the Smart City areas have also implemented a Smart City Cybersecurity lab to test the technology in the Smart City.

The result also indicate that all the Smart City areas work with policy, regulatory and legal solutions. The result implies that there are policy, laws and regulations on national level that the Smart City areas need to follow. The Smart Cities also have regulations for their vendors and one area mentioned that they also have policies and agreements towards the users in the Smart City. In addition to this the result show that education and training is nothing that is used in non of the Smart City areas when it comes to security and privacy in Smart Cities.

Overall, these results indicate that all the cities work with governance and management solutions. According to the respondents is it essential to have a plan for the security and privacy in the Smart City however when it comes to objectives and goals this is nothing they work with. The result also indicates that the vendors of the technologies in the Smart City have a huge responsibility for the security and privacy. The result show that all the Smart City areas work with experts or have a security/privacy team and some the Smart city areas have some kind of city emergency response team. The result identify that it was just one Smart City area that have a privacy and security board.

5 Discussion

Chapter 5 aims to discuss how literature and empirical results connect to one another. The discussion follows the same structure as chapter 4 and our research model. Therefore, the headings of this chapter consist of the four concepts.

5.1 Security challenges in the Smart City

Most of the security challenges discussed in the literature review are related to technology and according to the empirical results this is still the case.

In contrast to the literature review where cloud services are considered a security challenge related to Smart Cities, this was not identified as a challenge by any of the respondents. However, one of the experts mentioned cloud as the biggest challenge in the Smart City (Appendix 1: 53). Zhang et al. (2017) describe that cloud services faces security threats due to the untrusted cloud servers and there are different suppliers of cloud services which leads to that different standard's complicate matters regarding privacy and security. Other authors (Braun et al., 2018; Baig et al., 2018) also points on the security risks with cloud services. A possible explanation for why cloud is not considered a challenge among the respondents might be due to the benefits of cloud storage that are described by Braun et al. (2018).

5.1.1 Connectivity

The empirical results indicate that connectivity is a security challenge. When many pieces are put together in the Smart City it can create holes in the system. This is consistent with what Edwards (2017) writes about Smart Cities being complex systems that rely on integrated communication systems. Which can lead to that if you have one weak link it can lead to that the whole system being insecure (Edwards, 2017).

Braun et al. (2018) describe that interconnectivity is a characterizing factor in a Smart City that leads to data being transferred and utilized through the entire Smart City processes. Although, what Braun et al. (2018) mention is presented under the paragraph Privacy challenges in Smart Cities. Kitchin and Dodge (2017) describe that Smart Cities are complex, large and diverse systems with a lot of interdependencies and this makes it hard to know how all components are exposed, to ensure end-to-end security. This is, however, related to the third vulnerability of technologies in a Smart City that can be exploited by attackers. Furthermore, connectivity is discussed as a challenge in the literature review, even if it does not have an own section, and it is mentioned among our respondents which makes connectivity a security challenge that needs to be considered when implementing Smart City initiatives.

5.1.2 Internet of Things

As mentioned in the literature review, IoT is the enabling technology in the Smart City and the Smart City includes several types of IoT sensors (Baig et al., 2017). The vulnerability and insecurity of Smart City systems deduces from the known familiar lack of security and trustworthiness of the IoT in general (Ijaz et al., 2016). One respondent mentioned that security is not added to IoT and that makes them a vulnerable place regarding security (Appendix 4: 34). Popescul & Genete (2016) describe that it is common that designers let security aside when designing IoT applications and they hope it could be added later-on and attack-resistance is most often losing against other design factors. This is consistent with what one of the expert stated that security might first be insufficient but later on some might start thinking about it (Appendix 1: 86).

IoT is something that both the literature review present (Baig et al., 2017; Edwards, 2017; French & Shim, 2016; Shim et al., 2019) and also respondents from different areas discussed which makes it a security challenge that definitely needs to be considered. It can be noticed that IoT is a topic that is continuously brought up and the security and privacy challenges around the technology in the Smart City needs to be further considered and tackled.

5.1.3 Secure Data

Four of the respondents stated secure data as a security challenge. Due to all the data about citizens, it was described that it is crucial to have secure and anonymized information (Appendix 2: 28). Secure data is discussed in the literature review, both under security challenges and under privacy challenges. Shim et al. (2019) states the challenge of securing the information flow that comes from the IoT devices and under privacy challenges it is written that the two biggest fears humans have with big data is the security of this data and the personal privacy (Demirkan et al., 2015). Aldairi & Tawalbeh (2017) discuss that privacy is ensured by protecting identities that indicate protecting personnel and their confidential data and Li et al. (2015) describe that one of the most difficult challenges in a Smart City is to secure sensitive data.

Edwards (2017) also describes that the costs of storage and processing of data have dramatically fallen, and Smart Cities are both consumers and producers of Big Data. Due to this data that is generated through Smart City infrastructure and because of the fears related to big data, it is a given that all respondents from two areas, that also are on different maturity levels, see securing data as a challenge and it should further be considered a challenge that needs to be tackled in Smart Cities.

5.1.4 Cyberattacks

Kitchin and Dodge (2019) write that cyberattacks try to exploit one of the major vulnerabilities that are central to the Smart City systems. Smart applications are also exposed to hacking through up-to-date attacks (Cui et al., 2018). Cyberattacks is nothing that anyone of the respondents mentioned that they have been exposed to. Furthermore, even if they say they have not received any cyberattacks, it is noticeable that all respondents know of the consequences that can come from a cyberattack.

The empirical results presented that in some cases there could have been hackers that have tried to attack their Smart City systems, but the respondents do either not have the knowledge about it or there has been strong security so the attacks have not been successful. Furthermore, cyberattacks should be considered a security challenge since respondents from all areas recognized consequences related to cyberattacks even though most of them have not been exposed to a cyberattack.

5.1.5 Lack of knowledge and awareness

Security challenges related to users was brought up by three respondents and two experts and the common thing was that all mentioned a lack of knowledge and awareness as a challenge. Lee et al. (2019), Harbers et al. (2018) and Shim et al. (2019) recognized security challenges related to users and that there is a lack of knowledge and awareness among users, IoT producers and among policy makers. Harbers et al. (2018) state that when information systems become better protected, attackers shift focus and attention to human elements to break into these systems.

Although lack of knowledge and awareness is considered a security challenge among respondents from all areas, no one mentioned directly that they educate and train employees and users to be aware of the security risks with the systems. Lack of knowledge and awareness should be considered a security challenge and appropriate solutions, for instance education and training, can be implemented to tackle this challenge.

5.1.6 Security is not considered an issue

The empirical results indicate that all the respondents except for one are aware about the security challenges in the Smart City. This respondent mentioned that security is not considered a challenge in the organizations and security is nothing they discuss in the organization. A possible explanation for why this respondent did not see security as a challenge could be because the respondent mostly works with sustainable cities and not Smart Cities. However, this is also an important finding, because according to Marsal-Llacuna et al. (2015) most sustainable cities are moving towards Smart Cities and then they need to start thinking about the security and privacy aspects. The respondent describes that a reason for why they do not talk about security in the organization is because instead people want to innovate, come up with new solutions and implement them on the market (Appendix 6: 70). This is in accordance with what one of the experts mentioned but also Edwards (2017) and Ijaz et al. (2016) that the functionality is more important than the security and there is a bigger interest in implementing the product than thinking of the security and privacy aspects.

In addition to this, some security challenges that are presented in the literature that are not mentioned by the respondents include smartphones, smart grids, cloud services and artificial intelligence. The reason for why respondents does not mention artificial intelligence (AI) as a challenge can be due to that AI is still not a fully developed concept in Smart Cities. For instance, Braun et al. (2018) describe that Smart Cities will rely on automation for efficiency and for implementing automation, AI will be critical, and he describes it in a way that it is not implemented yet. Although, some respondents recognized consequences related to, for instance, smartphones that collect a lot of location data (Kitchin, 2016) which can lead to tracking people's behaviour, but they do not directly mention smartphones as a security challenge in the Smart City. We believe that lack of security testing is not a security challenge because no one of the respondents mention this as a challenge instead they described how they work with security testing, this will be described further in paragraph 5.4.1.

5.2 Privacy challenges in the Smart City

As described in our empirical results for privacy challenges (paragraph 4.2), privacy challenges were more discussed as a consequence and how people's privacy can be affected when, for instance, security breaches occur. Therefore, this chapter is not discussed to the same extent as the other three concepts since consequences is further discussed in paragraph 5.3. Another reason for this is because the empirical results indicate that most of the Smart City solutions do not handle sensitive data today and is therefore not considered a challenge in the same degree as the security challenges. We still believe that they need to consider the privacy challenges when implementing Smart City solutions.

Braun et al. (2018) describe that privacy threats in data sharing and data mining exist, and the interconnectivity means that multiple parties communicate and gain access to information and between different stakeholders it can differ in priorities which leads to gaps between privacy standards. Smart City systems can also combine different data sources and one respondent recognized this as a challenge related to privacy when data sources are being combined in a way that they did not thought was possible (Appendix 2: 39) and this is one thing that Mai (2016) also describes.

The results indicate tracking people and their behaviour as a challenge related to privacy. Several studies (Kitchin, 2016; Li et al., 2015; Elmaghraby & Losavio, 2014; Ijaz et al., 2016) discuss the problem about locational data and data about people's activities and profiles. For instance, Kitchin (2016) describes that smart technologies have transformed location and movement tracking to a case where monitoring of location is automatic, continuous and relatively cheap.

Privacy challenges can be in terms of the use of cameras, GPS, information that is linked to people's behavior and how they move in the city and is mentioned by one respondent (Appendix 6: 28). According to Kitchin (2016) cities use different smart technologies to monitor and control activities, for instance sensor networks, CCTV cameras, GPS in vehicles and smart card tracking in buildings. Elmaghraby & Losavio (2014) describe that automobiles and their systems can be a great source of data about people's activities and locational data can detail a lot of a person's life that they do not wish to reveal. This is consistent with what another respondent also described about being tracked with cross-coupled information (Appendix 4: 18).

One respondent brought up the challenge of being aware of when you are breaching the privacy and it is important to know when you are going too far and breaching privacy (Appendix 9: 38). For instance, Smart Cities are both consumers and producers of Big Data and data is generated through traditional city infrastructure and complemented with big data from private companies (Edwards, 2017) and this data will increasingly be combined by public city managers and private service providers (Demirkan et al., 2015). Due to this increase in data that are being generated, both private and not private data, it is a given that some respondents consider it a challenge about being aware when privacy breaches are done. However, this challenge can be related to the challenge of lack of knowledge and awareness presented in security challenges.

5.3 Consequences of security and privacy challenges

Consequences that can happen as a result of inappropriate security and privacy solutions are discussed under this section.

5.3.1 Loss of critical systems

According to the empirical results, a consequence of the security challenges was loss of critical systems in the infrastructure. This consequence was also identified by Ijaz et al. (2016). According to Ijaz et al. (2016), changing a single process in a critical system can cause delays or loss of services. The empirical results found that the functions in the city that would create the most damage in the city is the loss of electricity and the loss of internet, and that could have very bad effects for the city and the citizens. Other vital functions that the respondents mentioned that could create damage in the city is the loss of mobility and loss of water. Aldairi & Tawalbeh (2017) agree with that loss of mobility can cause catastrophes especially when they happen in air traffic systems, train control systems or the road signs and speed limit.

The literature review also presented that the security and privacy challenges could have consequences for the banking and finance business area, however this was not identified in the empirical results.

5.3.2 Datafication

Kitchin (2016) presents that various privacy breaches can happen in a Smart City environment as an effect of lack of appropriate security. One of these are surveillance which refers to watching, listening or recording an individual's activities. Surveillance is a consequence of security that all the experts mentioned as did several of the respondents. The threat to surveillance is especially when the cameras are implemented in the Smart City, the respondents explained. Kitchin (2016) as well as Aldairi & Tawalbeh (2017) stated that there is a challenge with the cameras because the cities are full of private and public cameras and reaching these cameras and have access to them can cause violation to individuals' privacy. The biggest challenge with cameras and surveillance is that someone can track other people and find out patterns for the individual citizens for example where they live or what metro they take (Appendix 1:74).

5.3.3 Loss of trust

Kitchin (2016) describes that the privacy breaches that can happen in a Smart City environment can be surveillance, distortion, identification and aggregation and if these privacy breaches are made it can affect the trust among the citizens. Edwards (2017) also writes that big data is generated through city infrastructure and it can both be private and not private data but if this data is used in the wrong way it can lead to a lack of trust among citizens and users. This is consistent with the results of this study. A consequence that was identified in the empirical results is the lack of trust in the Smart City if a cyberattack or privacy breach would happen, and sensitive information would be revealed. If something happen the citizen's trust of the Smart City solutions can be destroyed. The results found that another consequence of this is that the citizens will be against implementing more Smart City solutions and it will be harder to run Smart City projects. Therefore, it is very important that the Smart City work with security and privacy so this will not happen, and the trust will disappear. If the citizens do not trust the Smart City it might also lead to that they refuse to use the systems as intended and that the Smart City becomes obsolete (Braun et al., 2018).

5.3.4 Misuse of data and physical harm

The results indicate that lack of security can lead to both misuse of data and physical harm to the citizens. Several of the respondents mentioned that if the system is hacked because of lack of security it could lead to that criminals can do evil things that can benefit their own purpose. They can misuse the data for things that was not the purpose when the data was collected. According to the respondents the data can be misused to send out advertisement or even to change healthcare information.

Another important finding was that the misuse of data also could lead to physical harm for the citizens. For instance, one of the experts explained if the healthcare data is changed it could lead to that people get the wrong medicine and that could lead to death for the citizen. These results reflect those of Ijaz et al. (2016) who also discussed that if the healthcare sector is prone to security threats it cannot just cause privacy concerns of a patient but can also pose threats to a person's life if critical information is changed by the attacker. Another finding of when modification of data can lead to physical harm is if someone for example hack the system in smart cars, this could lead to changes in speed or the distance and this can cause physical harm for the citizens. This finding seems to be consistent with that of Aldairi & Tawalbeh (2017) who described that hacking speed limit signs, road signs and traffic lights could lead to huge traffic jams and road accidents that will last for hours and similar consequences could happen if the smart car is hacked. Li et al. (2016) also discuss that if an attacker gets access to the traffic light systems, they can eavesdrop on traffic and even control the traffic lights.

5.4 Solutions to security and privacy challenges

As mentioned in the literature review most strategies adopted for securing Smart Cities have mostly been technical mitigation solutions (Kitchin & Dodge, 2019). The empirical results of this study differ from that since in all the Smart City areas investigated, they work in addition to the technical solutions with policy, regulatory and legal solutions and also management and governance solutions to make the Smart City secure. The result also indicates that there is not one single solution that is more important than another, and they cannot look at things isolated in the Smart City. This result may be explained by the fact that it is important and necessary to have other solutions than just technical solutions to secure the Smart City according to Kitchin and Dodge (2019). This finding is consistent with Kayworth & Whitten (2010) findings who reported that while technology is still essential for security it represents just a part of an overall solution that must include other organizational elements of the business to create an effective information security. Since the results found that all the Smart City areas knew about the security and privacy challenges with related consequences, it is therefore possible that they have understood what Kitchin and Dodge (2019) and Kayworth & Whitten (2010) present as important to have an effective information security and to secure the Smart City.

5.4.1 Technology solutions

Best practice

Technology solutions to security and privacy challenges consists of implementing best practice solutions in creating and maintaining secure Smart City systems and infrastructure according to Kitchin (2016). The empirical results indicate that all Smart City areas work with firewalls and two of the areas also work with data encryption, which is a best practice solution according to Kitchin and Dodge (2019) and is implemented to make sure that there are no weak links between components. Furthermore, it is unclear if the Smart Cities have implemented firewalls in every transition point, which is of importance to handle the security challenges in the Smart City (Khatoun & Zeadally, 2017; Presley & Landry, 2016).

In addition to this, respondents from two of the areas mentioned that they work with people's access control to the systems in the city. Strong access control is a best practice according to Kitchin (2016). It is of importance that the cities work with this because threats of unauthorized persons accessing the system inside the Smart City without special authentication is a security challenge according to Lee et al. (2019). To have control over people’s access control is crucial since, according to Kitchin and Dodge (2017), there are multiple vulnerabilities arising from human error.

Another important part of the technical solution is to ensure full backup of recovery mechanisms and data (Kitchin, 2016). One area work with this as well. They have two servers and data is added on the server every night, so there is full backup all the time (Appendix 4: 16). One of the servers have cloud service as well so there is always back-up (Appendix 7: 46). However, the respondent do not mention any security risk with the cloud service and in this case it is seen as a solution, which is contradictory to what one expert (Appendix 1: 53) explained and literature review (Baig et al., 2018; Zhang et al., 2017; Braun et al., 2018) mentions.

The empirical results show that all areas work with trying to follow an architecture for security. Two areas mentioned the importance of having data and information infrastructure for the collection, sharing and how to handle the data. Another area tries to build a reference architecture of what kind of security measures that are needed when they implement Smart City projects. These results reflect those of Harbers et al. (2018) that describes the importance of having infrastructure that is pervasive interoperable and intelligent at all system levels, including the architectural level.

According to the empirical results, one Smart City area mentioned that they use standard components from the industry when they build their Smart City systems. Standard and security protocols are as well used in their projects according to the respondents (Appendix 3: 8). Kajtazi et al. (2018) discuss that standardization in itself can be hard in an environment like Smart City that pose a lot of complex and interconnected technologies. Hence, even if they buy standard components from the industry it can still be difficult to implement these in the Smart City and make that standardized.

Security testing and Smart City cybersecurity lab

As presented in the literature review, one security challenge related to the technical factors is that the governance authorities, the customers of the technology do not test the systems based on the security factors when they buy the technology and implement the technology in the Smart City (Ijaz et al., 2016; Edwards, 2017)**.** As discussed in security challenges, according to one of the experts many private companies do not think about the security and privacy aspects when they develop technologies to the Smart City. It is therefore very important to test the technology before it is implemented in the Smart City. The empirical results indicate that all the areas investigated work with some security testing, but at different levels and in different stages of the projects. The results found that in the areas in maturity level three they started with the security testing after the pilot tests had started. A possible explanation for this could be that the governance authorities believe it is more important to test the functionality than the security, which is a bad prioritization according to Ijaz et al. (2016). However, in one of these areas they have understood how important the security is, so they have started a project that is fully focused on security and they use a security lab to test the technologies (Appendix 4: 10).

One interesting finding was that the Smart City area in maturity level four has established a Smart City cybersecurity lab at the technical university where they work with the security and privacy challenges in their projects. Another interesting finding was that in addition to the Smart City cybersecurity lab, the same area has launched some hackathons where they test the security in the systems. This could be an idea for the other Smart Cities since one of the respondents mentioned that it would be quite fun if someone would try to hack their systems because then they learn and today is the data not so sensitive so no damage would be made if they were hacked (Appendix 4: 28).

A reason for why only the Smart City in maturity level four has implemented a Smart City cybersecurity lab could be because they are the only Smart City that have implemented a Smart City solution in the city yet and they therefore had a need to test the solution more than the areas in maturity level three. Implementing a Smart City cybersecurity lab could be a further development in the Smart City areas in maturity level three before they implement a Smart City solution and go to maturity level four.

According to the results, we can infer that there is not a lack of security testing, because they do not implement anything in full-scale in the Smart City before they have tested the technology. A possible explanation for why there is no lack of security testing may be that the results indicate that much of the responsibility for security and privacy is on the vendors that develop the technology. Since the result also indicated that there is a risk that many private companies just care about functionality and not about the security, it is therefore necessary that the Smart City test their solutions before they are implemented the city.

Blockchain and Artificial Intelligence

According to Biswas & Muthukkumarasamy (2016) blockchain technology can be used in the Smart City to secure that it is resilient against many threats. Blockchain is also discussed as a solution to security challenges in IoT (Shim et al., 2019). Blockchain as a solution to the security and privacy challenges was not discussed by any of the respondents. However, another advanced technology is Artificial Intelligence and one of the respondents mentioned that in the future there is an idea that AI can be used in the Smart City as a system that can learn when new sensitive data is added to the system (Appendix 4: 52). AI can therefore be a solution to the challenge with cross coupled information, that was identified as a privacy challenge. The AI system can understand how data can be combined and can avoid data to be combined so sensitive information can be created. The empirical results also found that there cannot be people that analyse the data and therefore the AI system can be used to make sure that the data is correct in the system. Something that is of importance for security controls is intrusion detection software according to Presley & Landry (2016) and AI could be used as an intrusion detection software in the Smart City. However, the results indicate that when implementing AI in the Smart City new security risks can appear (Appendix 1: 55 & 56).

5.4.2 Policy, regulatory and legal solutions

How the technical solutions are administered is framed by the wider policy, regulatory and legal landscape (Kitchin, 2016). Several of the respondents mentioned that they have policies and regulations that they need to follow in the Smart City, but they also have requirements on the vendors. There are rules on national level that the Smart Cities need to follow like GDPR and there are also laws that the private companies that develop the technologies need to follow when it comes to security and privacy.

Another interesting finding is that in one of the areas they also have regulations and policies for the users of the Smart City, the citizens (Appendix 3: 36). Two of the respondents mentioned that they use policies and agreements to the users in the Smart City. In one of the projects each individual also needs to sign that it is okay for the company to collect the private information (Appendix 4: 20). A possible explanation for this could be that they give away some of the responsibility for security and privacy to the users. However, this could create a lot of damage since the identified security challenge lack of knowledge and awareness from the users. The users can accept the agreements without knowing what it means in practice. If the users get the responsibility for the security it is also necessary that the Smart City makes sure that they know what it means.

The results found that the policies, regulations and legal aspects are an important part to secure the Smart Cities. The result also indicates that the private companies that develop Smart City applications do not think about security and privacy. Therefore, it is essential that there are laws and regulations for how the private data must be handled both for the private companies but also for the Smart City. The regulations and policies are a way for the Smart Cities to work with prevention, to secure the Smart City system, something that was identified by Kitchin (2016) as an important part. However, according to the empirical results the private companies do not always follow the legal aspects for security and privacy (Appendix 1: 101). The Smart Cities could therefore not trust completely, that because there is a law or policy for how to handle the security and privacy it is not clear that they follow these laws. In addition to this, one interesting point is made by one of the respondents. Even if they have all these agreements between the Smart City and the vendors and private companies, if a cyberattack or privacy breach would happen to the Smart City system it does not matter what is written in the contract, the catastrophe will still happen in the city (Appendix 7: 40).

Privacy and Security by Design

Privacy by design is an approach to protect privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure (Edwards, 2017) and the default mode of operation and when collecting data (Kitchin, 2016). Security by design is complementary to privacy by design and it seeks to build security into systems, instead of layering it on as an afterthought (Kitchin, 2016). The results found that all the Smart City areas work with security and privacy by design, but the respondents describe how they work with it in different ways. In two of the areas they described that they think about security and privacy from the beginning in their projects which is consistent with security by design described by Kajtazi et al. (2018). Security should be built in from the beginning and not added as an afterthought (Kitchin, 2016). The results also indicate that they try to not handle private data in the Smart City solutions when it is possible and when they do this, they can filter the data to remove sensitive data. Furthermore, Kitchin (2016) states that in security by design the security measures should be tested before the product is launched. There is just in one of the areas that a project has been launched which is not in the pilot stage. However according to the empirical results this area tests the product before it is implemented (Appendix 4: 93).

Education and training

As mentioned in the literature review, it is important to educate and train the users on how the technologies work and how to handle the security and privacy challenges in the Smart City (Kitchin, 2016). The empirical results showed that education and training is nothing that the cities work with when it comes to security and privacy in the Smart City. The empirical results presented that in one area they have worked with education of how to use the Smart City solutions, and in another they have had training about how to use networks and how to connect to sensors, but no one of these are related to security and privacy in the Smart City. The results found that the Smart City areas have had training or plan to have that with the users, however this training is either focused on security and privacy or the Smart City, never on both parts.

In relation to this, one of the security challenges found in the empirical results is that it is common that employees are not very used to technologies and do not have the right education which can result in security risks (Appendix 8: 66). It was also identified that the employees need to have insight about the security challenges. This result reflects those of Kajtazi et al. (2018) who also found that training and education is needed to raise awareness regarding IoT systems, challenges and risks. Because IoT systems are a big part of the Smart City this is also important in the Smart City. Kajtazi et al. (2018) also discuss that both regulators, policy makers and the general public should be included in this education since awareness and security education is needed for both developers and the users of the smart products. In accordance with Kajtazi et al. (2018), a privacy challenge identified in the empirical results is that it is important to be aware of when you go too far with the applications and breach the privacy and some respondents also consider it a challenge about being aware when privacy breaches are made.

The finding that there is a lack of education may be explained by the fact that the empirical results showed that educating the employees is one of the things that take the most time and resources relating to security and privacy in the Smart City. However, it is necessary that the Smart Cities work more with education and training for both the employees that will implement and use the technologies but also for the users to make the users aware about the risks. In this way Smart Cities can decrease the lack of knowledge that was identified as a security challenge both in the result and by Lee et al. (2019). As mentioned in the literature review, the education and training should be customized between the users because it will be more effective than generic training (McLaughlin & Gogan, 2018). Harbers et al. (2018) also discuss the importance of investments in education for the future generations of users and developers of the Smart City systems. This was nothing that was identified in the empirical results and something the Smart Cities could work with in the future.

5.4.3 Governance and management Solutions

Leadership and planning

Kitchin (2016) writes that Smart Cities are often developed with little coordination regarding security and privacy harms and Presley and Landry (2016) implies that cybersecurity management is needed through the entire lifecycle. Despite what Kitchin (2016) is writing, four respondents, representatives from all three Smart City areas, stated that they need to have a plan and identify risks before they start with a Smart City project. One of the respondents for instance mentioned that before they start a project, they go through what kind of risks there are, and especially if personal data is involved (Appendix 9: 66). Another respondent gave the example that they information-classify the information, they evaluate how sensitive the data is before they start to collect data (Appendix 2 :30). To bring in security questions into the projects that are performed is something that one of the respondents mentioned that they always do (Appendix 2: 71). McLaughlin & Gogan (2018) discuss how it is possible to prepare for information security incidents and from the empirical results it is found that all Smart City areas investigated focus and plan for security in some way.

The empirical results also indicate that when new technologies are used in the Smart City it is important that they plan for this, so they have enough time and resources to make them secure. One example of this is that when cameras are implemented in the Smart City one respondent explained that this will be something that they need to work a lot with. The camera technologies collect a lot of sensitive data and they need to figure out how to use the cameras in the right way. Since the camera technology also collect a lot of sensitive data it is very important to make these secure. However, no solutions of how to handle surveillance more than trying to eliminate as much personal data as possible have been identified in this study.

Related to this Kajtazi et al. (2018) state that security is a continuous process. The empirical results also indicate that one of the hardest challenges with security is that security of a system is never finished, and you always need to continue to work with the security, which is something practitioners need to consider. New things always show up and people find new ways to hack the systems and there could always come new risks. This is consistent with Dorasamy et al. (2017) who state that attackers are moving fast and cyberspace is a goldmine for crime and violations. In accordance with this the results show that a challenge with security is that they always need to work with it and security has never an end.

Objectives

To have security incentives and objectives that copes with the complexity of the system and to increase knowledge among users and stakeholders are critical for the ones responsible for the Smart City initiatives (Harbers et al., 2018). Despite this, the empirical results showed that goals for security and privacy is nothing that is defined in the Smart City, neither of the areas work with goals for security and privacy. The reasons for this were that one of the respondents stated that they do not have any goals for security because security is not an issue while another respondent stated that they do not have any goals for security since it is something obvious. Harbers et al. (2018) describe that incentives related to supply chain can help making a Smart City more secure since various parties are often involved in the creation of these systems and from the results it is noticeable that there is a lack of these incentives. This result may be explained by the fact that the empirical results showed that neither of the areas have a Smart City advisory board. According to Kitchin (2016), the Smart City advisory board is responsible for the strategic visioning of the composition and a board like this could create strategic goals for security and privacy in the Smart City. To have goals or objectives related to security and privacy in the Smart City could lead to that people are more aware of the risks related to security and privacy in their city. This could lead to that the challenge related to a lack of knowledge and awareness, which is a security challenge both according to the literature (Lee et al., 2019; Harbers et al., 2018; Shim et al., 2019) and the empirical results, are being managed and decreases in the Smart Cities.

As described in the empirical results, much of the responsibility for security and privacy is on the vendors according to our respondents. Because of this, it would be obvious to have clear incentives or goals related to security and privacy since it could increase stakeholder's awareness and make sure that all parts work to reach the same goals when it comes to security and privacy.

Experts and security/privacy team

According to Kitchin (2016), the core privacy/security team should undertake the work within the framework dictated by the governance. The empirical results showed that all of the Smart City areas work with experts in security or have a security/privacy team. The explanation to why the areas works with experts and security teams are that they do not have the knowledge by themselves, according to the empirical results. Although, no one of the respondents are completely clear on what these experts and teams actual work-tasks are and Kitchin (2016) describes that a security/privacy team's work includes for instance undertaking threat and risk modelling, testing the security of Smart City technologies and coordinating staff training on privacy and security challenges. Furthermore, even if Kitchin (2016) describes it in this way we interpret that since most cities are outsourcing security, they rely on these companies and that they develop secure solutions. Although we believe that relevant and clear security objectives would be needed when these type of outsourcing is done to make sure that they work against the same goals.

City emergency response team

CERTs are emergency response teams that tackle city events (Kitchin, 2016) and the empirical results presented that all cities have a team which is responsible if an emergency happen. Although, this team might be more similar to an emergency response team that tackles city events than a team focusing on Smart City initiatives. Kitchin (2016) writes that a CERTs consists of key personnel from IT services, the core privacy/security team, Smart City initiatives and emergency services and CERTs are handling problems when Smart City technology experience a cybersecurity incident. The respondents mainly stated that they have crisis management in the city, so even if this is not especially related to the Smart City, these crisis teams will be able to handle a crisis even if it is caused by a Smart City solution. The empirical results found that the collaboration between the Smart City team, the core privacy/security team and the emergency team could be improved because then they can learn from each other and the security and privacy in the Smart City can gain advantage from this.

Security and Privacy Board

A Smart City governance, ethics and security oversight committee focus includes, for instance, to certify that the city's Smart City strategies are being implemented and meeting targets and that they conform to legal and regulatory requirements and ensure there is clear communication to public concerning how the Smart City is being realised and how data are being generated, used, stored and shared (Kitchin, 2016). No one of the respondents mentioned anything about a committee but in the area in maturity level four they have a board that discuss different kinds of problems related to privacy before they roll-out a digital solution (Appendix 5: 50). A possible explanation to why not any of the other Smart City areas have a board for the Smart City projects, may be because they have not implemented anything yet and they have not come so far with their Smart City projects as the area in maturity level four. However, in the future it could be relevant for them to implement a security and privacy committee related to the Smart City to discuss the security and privacy challenges.

5.5 Implications to research and practice

To summarize the discussion from two perspectives in terms of implications to research and practice, in the section above we have tackled our empirical results that challenge prior work. Below we provide our implications in a summarized form as an output of this thesis.

5.5.1 Implications to research

In this thesis we have identified different aspects that needs to be further tackled. First of all, we identified that it needs more research about how Smart Cities handle the security and privacy challenges related to cloud solutions. Other aspects that needs further investigation includes how the Smart Cities work with objectives and also education and training to improve the security and privacy in the Smart City. Lack of knowledge and awareness was an identified challenge in this thesis and more education and training on security and privacy could decrease the effects of this challenge. However, further research is needed on this challenge to investigate other possible solutions as well. The result indicates that there is not a lack of security testing, however more research could be the improvements a Smart City cybersecurity lab could have on the security and privacy aspects in Smart City initiatives.

5.5.2 Implications to practice

In this thesis, we have identified that there is not one single solution that is more important than another, instead all the solutions are important together. Smart Cities cannot look at things isolated, they need to see everything in collaboration. The empirical results also indicate that one of the hardest challenges with security is that security of a system is never finished, and you always need to continue to work with the security, which is something practitioners need to consider. Moreover, it is identified that practitioners need to work more with education and training to raise the awareness of security and privacy challenges in the Smart City. The thesis also identified that planning is needed from the beginning, but the results also indicate that there is a lack of clear objectives when it comes to security and privacy in the Smart City.

6 Conclusion

The purpose of this thesis focused on investigating in what ways Smart Cities work with security and privacy challenges. In doing so, the thesis determined the need to tackle security and privacy challenges that occur in a Smart City, by also tackling the consequences that can arise because of these challenges. Thus, this thesis initiated the following research question: *In what ways do Smart Cities work with security and privacy challenges?* which we will answer below.

While security and privacy challenges were extensively tackled as identified from the empirical setting, one important aspect to be highlighted is that Smart Cities do not only work with technical solutions in respect to security and privacy, a general understanding found in the literature. The technical solutions are still an important aspect for understanding in what ways Smart Cities work with security and privacy challenges. However, exploring the empirical setting, we identified that Smart Cities also work extensively with both policy, regulatory and legal solutions, and governance and management solutions, surpassing the agenda to focus on technical solutions alone. Thus, the results of this thesis complement those of earlier studies by pointing out that researchers and practitioners should not only consider the technical solutions for security and privacy challenges, but also other type of solutions. Solutions that are more strategic in nature when it concerns taking decisions about how, what and why certain security and privacy solutions should be introduced. One important result of this thesis is to show that Smart Cities were aware about the security and privacy challenges and the related consequences these could lead to, therefore they work in this was with all these kind of solutions.

Nevertheless, this thesis also finds that the technical solutions continue to be of prime importance and that they include the use of best practice solutions and security testing. The results show that the future technical solutions could include AI as a way for the Smart Cities to work with security and privacy challenges.

The policy, regulatory and legal solutions incorporate security and privacy by design which is identified as a way that all the Smart City areas work with. Another policy, regulatory and legal solution is education and training, but this is not identified as a way the Smart City work with security and privacy. Furthermore, this thesis finds that there are several policies and regulations that Smart Cities need to follow, and these are an important part to secure the Smart City.

The governance and management solutions consist first of all of strong leadership and planning. Planning for security and privacy is identified as a way that all the Smart Cities work with. All the cities also work with experts or a security/privacy team which are the experts that have the knowledge about security and privacy in the Smart City. Another way of how they work with security and privacy challenges is that all the areas have a kind of city emergency response team. Although, this team might be more similar to an emergency response team that tackles city events than a team focusing on Smart City initiatives. One more way of how to work with security and privacy challenges is to have a Security and Privacy board, this thesis found that it was just one of the areas that have a board like this. However, objectives are not identified as a way of how the Smart City work with security and privacy challenges.

To conclude here, this thesis does not find one single solution that is more important than another, but instead suggests that all the solutions are important together when tackled together.

6.1 Key findings

This study has identified in what ways Smart Cities work with security and privacy challenges and the key findings of this study will be presented here.

Security testing and Smart City cybersecurity lab
Security testing was identified as a way to make sure that the Smart City systems are secure. Security testing is of importance since it was described that they work with a lot of different vendors and how they work with security and privacy and what standards for security they have can vary. Security testing is of importance because of all the technical security challenges that were identified. One significant finding from this study was the Smart City cybersecurity lab, a lab that is completely focused to test the security on Smart City initiatives. This lab is a new identified way on how to work with security testing for Smart Cities and a lab like this could be implemented in more Smart Cities.

Education and training
Lack of knowledge and awareness was one of the major findings related to security and privacy challenges in a Smart City. It was clear to see a correlation between this challenge and that there also existed a lack of education and training about security and privacy in the Smart City. Although, this is not how the Smart Cities work with security and privacy challenges today, but education and training should be a way of how they work with eliminating challenges. The lack of knowledge among employees can have significant consequences for the Smart City, so it is important that Smart Cities implement education and training about security and privacy in a Smart City for the employees but also for the citizens.

Objectives
Objectives was not a way that was identified on how they work with security and privacy challenges today. However, it could benefit the Smart Cities if they worked with objectives related to security and privacy in a Smart City since in the Smart City there are so many stakeholders involved in initiatives. Objectives could also affect the knowledge and awareness among employees but also to make sure that all stakeholders work against the same goals and should therefore be a way for Smart Cities to work.

Strong leadership and planning
Due to the security and privacy challenges that arise in a Smart City environment it is crucial that Smart Cities plan for how to handle the security and privacy, from the beginning and throughout the entire lifecycle. It is of importance to identify the security risks and what data that are being collected which affect the privacy concerns. This is a way of how the Smart Cities work with the security and privacy challenges today.

Security should not come as an afterthought and security questions should be brought up in the beginning phase of a Smart City initiative. Something that is important to point out is that security is never finished and should be seen as a continuous process, therefore it is not enough to just think about privacy and security in the beginning but also during the entire project and as well for the future. Because the security threats will change, and Smart Cities need to stay updated on how to tackle the security and privacy challenges. Most of the respondents have not implemented a full-scale Smart City initiative but to continue working with security and privacy questions after they have been implemented is a way to tackle the security and privacy challenges.

6.2 Future research

For future research, it was identified that how Smart Cities handle the security and privacy challenges related to cloud solutions needs more research. How the Smart Cities work with objectives and education and training to improve the security and privacy in the Smart City are topics that as well needs further investigation. Lack of knowledge was an identified challenge in this thesis and further investigation is needed for possible solutions to this challenge since this thesis only proposes education and training as a solution. Smart City cybersecurity lab was a surprising finding and future research must tackle how this could improve the security and privacy aspects in Smart City initiatives. Future research can also collect data from more Smart Cities in different areas than these of this thesis.

We hope that our findings can serve as a guidance for those aiming to implement Smart City projects about what the challenges with security and privacy in the Smart City could be and what these could lead to, but also in what ways they can work to handle the security and privacy challenges in the Smart City.

Appendix 1: Focus group interview

Job position: Researchers in security and smart homes
Located in Malmö & Lund
Date: 2019-04-12
Duration: 48 min
Language: English
Type of interview: Face-to-face

E1: Expert 1
E2: Expert 2
E3: Expert 3
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	So, it would be really nice if you could tell us what you work with and what you have done previously?
2	E1	So, okay, so I joined Malmö University as a PhD student here in August 2015 and my research is basically information security and privacy. And specifically, I am studying smart living and a case of that is smart homes. I have written a number of publications together with E2 and together with E3. That's it, but I also have a background in information security. Basically, I was a security manager for a number of years in a company based in Malta and so I had a team of four people working with me full time, information security officers. And basically, the banks where our clients, I won't say the name of the banks. Even some banks in Sweden.
3	E2	But also, you defended your thesis.
4	E1	Yes, so I had my defence in September 2018 actually and the thesis was about smart connected homes. We explored the security and privacy aspects of them basically. The risks and actually one of my... one of the first publications written here was about the exploration of security and privatization in smart homes actually which I think is maybe close to what you will be doing I would guess.
5	AS	Yes.
6	E2	So, I can introduce myself now. I am a senior lecture at Malmö University, and I have been here since 2015. My background is in computer science in general. Particularly, I work with internet of things and people research centre. Giving it aspects of open architecture, open systems. But what happened last year, I got to supervise one of the famous students, that you, we worked with him on a security topic. The idea was to extend my study of open architecture also to see what are the security aspects of this. And we did a joined work together with that student. We published a couple of papers and also, he was included to some of the activities we did here so that is more or less my background.

7	AS	Should we introduce our background/theory? Yes, like in our theory we bring up different technologies. We present... I can start with our research question instead, but we will investigate in what precautions or things like that, that cities are doing to prevent security and privacy issues. We have not decided a specific area, like smart mobility or smart governance or anything like that. But yes, we want to interview different cities like Copenhagen, Malmö and Lund, for example, so we can see if there is any difference between cities or if they are doing anything at all. For now, or theory is around information security and privacy, and like cyber security as well. And we also bring what challenges the literature bring up now and what solutions...
8	E2	So, what did you find so far from the literature?
9	AS	We found that like all of the techniques can be attacked from cyberattacks. And like Big Data, IoT, Smart Grids, RFID tags, Artificial Intelligence, all the techniques that are used in the smart city. And we have also looked at solutions and we talk about technical solutions and also... It’s like, policy and regulations solutions, and also governance solutions but from what we understand they have not truly been investigated and implemented, that we know of. So, we want like to see if any of these are implemented in the cities and if they have any other solutions that are not brought up in the literature.
10	E2	So, what is in short your aim, like one sentence? To just contextualize like the aim of your work is to identify challenges, security and privacy challenges?
11	AS	No, it’s like to find how they prevent...
12	E2	How to prevent security. Okay so it is about security mechanisms and stuff.
13	AS	So, we say that smart cities is built in smart mobility, smart living, smart people etc... what would you say is the area that has more security issues than the other one or do you have any experience
14	E1	sorry could you again.
15	AS	The smart city is built of six different components that we have found, smart living, smart mobility...
16	E1	Smart energy, I think.
17	AS	yes, smart environment…
18	E1	Smart governance
19	AS	yes, do you know if there is any of these areas that is more of a security risk?

20	E1	That depends, it is hard to answer that question it is. But, for example, smart energy can have a greater security concern than for example take a smart home for instance. Because you might affect the electricity of a country. You can for example have a text that black out the whole city for instance. Although, that is also possible to do with homes but the type of technologies used in smart living, used in smart homes, tend to be different than the technology used for smart energy, for instance. Although, they are becoming similar, they are connected to the internet and you need to have some kind of remoting system or if you have a smart building you need to control the temperature centrally. But the technologies are different, one is sort of industrial, the other one is consumer oriented.
21	E2	But there is a lot of security breaches from consumers perspective, especially if you take as an example, smart homes. So, I remember last year's paper when you presented in Athens and you did a study on...
22	E1	Cameras
23	E2	Cameras. So E1 run a very open and available script to access cameras. How many you have accessed?
24	E1	We found thousands of open cameras...
25	E2	And on those cameras, there were people, you could see them living, taking bath, kids playing. So, you could see them live. Maybe you could add that because this is also important
26	E1	and cameras or bot in private spaces, such as the home or closed but also in open spaces. So, you could for example find the camera in airport security, for instance. For sometimes at, I didn't find this myself, but like in these types of cameras. Which that you can find them, that is the big problem, because using readily available tools that everyone can access with very great ease. My mother that is not that technical can access this website, which is for example, then you find a filter which is already made, accessing cameras using default password. With a click on a button you get all of this information.
27	E2	So, it was thousands?
28	E1	yes, thousands.
29	AS	So, anyone could access these?
30	E1 & E2	Yes.
31	E2	Because vendors that develop these tools, they don't think about security neither privacy. They don't care, they just want the product to be out there. But then, they expose this different, if they don't have appropriate mechanisms, security mechanisms then. Of course, there is people that expose these devices. And yes, this is one of the issues I would say. And imagine if you take that technology and apply it in health. It is even worse because then, you have. You might have health issues and you

		don’t want to expose yourself or imagine if you are dependent on a certain IoT device that keeps your life up with that device. Because nowadays it might be common, someone might hack that device if there is a lack of security.
32	AS	Pacemaker.
33	E2	Pacemaker, yes.
34	AS	So, these are the ones that produce these, like develop them, they don’t think about security?
35	E2	There is a lot of small companies, they don’t think ahead about security and privacy. From the beginning, they start thinking about it later on. But the product is already available.
36	AS	How about the ones that buy the product and implement them? Do they try the product before they implement it or… from the security aspects?
37	E2	I don’t think so, especially small companies. They don’t think about security. At least based on our experiences.
38	E1	Absolutely, I have also seen some products and some companies, for example in China, who with the introduction of regulations, such as the GDPR. In order to process personal data, they need to comply with this regulation, GDPR, if they are opening for example in Europe. Now these companies, since they were processing sensitive data, they are out of business now. They decided to basically determine their product because they cannot afford to make their product secure, privacy preserving. So, regulations help but you need to afford them because you need to employ people, you need to have security staff.
39	E2	compliance, security thinking, design, security design and all these. These things are very important and before you start designing the product you need to think about security. So that then, the next step is to design the security mechanism before you implement it. This is the way of how it should be but usually this is not the case in today's industry.
40	AS	That is something that the literature talks about as well. Like security by design, privacy by design.
41	E3	Just to wrap up, also as a security expert you can perhaps even use that from a strategic point of view. To come back to your original question which is when you identify the six areas within smart work itself. You have some of the areas which are easier to tackle than some others, like smart energy versus smart living or smart home. Smart energy might have much higher challenges when it comes to security itself. Just the camera example, I think it illustrate very well on how that is applicable to any of these six areas. Whether a smart home where you identify that there is an open access camera or a child is in a crib, verses from a smart energy perspective where a camera is installed in to a nuclear power plant and that you can view what is going on right now. And when you think of the damage, how isolated it is in a smart environment if there is an intruder, it finds a security hole versus a power plant that can make a

		much larger damage. So here, damage to one family and one child but there, damage to one thousand children and one hundred thousand families or three hundred thousand children and one hundred thousand families if it is a three-member family. And also, the challenge is greater, the more complex that smart area is. That is what I would take from that if I illustrate it in other words.
42	E1	And also, what type of users. Like, for example, they would range from highly technical people to people which are low skilled in security. Take, for instance, homes then, for example, upgrading a camera software it might be difficult to perform by someone. That is a type of user. But then it might be someone working with smart energy, for example, and maybe more technical, so there is also that diversity between the users that generally they are the problem. So, we are not working in a technical environment where you have like highly skilled people who can help fix problems but if you are dealing with such a diverse you might have people that are not that technical.
43	E2	something related would also be like, as you mentioned, not technical skills. So, you have, and you bought it, let's say it is an IT product and things happen throughout the year and you still use that product but security mechanism has changed. So how does that user update his security, his device. So, I mean this is also about another problem which is about how do the companies or vendor make, kind off send notification about, some sort of awareness about that you need to update because we have this security aspect, there is new things coming up. Because hackers constantly, they will strive to access those devices. So, there is a need for new updates, new upgrades, new whatever. So how does it evolve, the security mechanisms. I think this is very.
44	E1	I would also use like the expectations. We expect like to have, to upgrade a product with a click on a button, like how we upgrade our phones. But it is not like that with IoT devices, sometimes it is just cheaper to throw it away and replace it rather than upgrading the software.
45	E2	But there is a lot of challenges when it comes to maintenance and evolution of these devices with security mechanisms because security changes as technology evolves.
46	AS	Of all of the technologies used in a smart city, which would you say have the highest risk to be threaten?
47	E1	It is difficult to say.
48	E2	Yes, if you can remind us again?
49	AS	IoT, Big Data, Artificial Intelligence, Cloud.
50	E2	I think…

51	E1	These are difficult questions.
52	E2	It is very hard to separate them because I think somehow, they are, these are interconnected. So, people constantly generate data. And that becomes big data. So, these things are connected to me at least. So, it is hard. I cannot say that this is the most, I don't know but what do you think?
53	E1	I most take like the cloud, for example, can be a bit, because you don't know what is happening inside the cloud or behind the cloud. So, for example, if you take the home, like most of the devices they are not that powerful to process the data that we have or that we need. Take an example with Amazon, that you sort of you having to have a keyboard, to interact with the device you interact with the voice. Now that device is not that powerful to process the voice so what it does. It sends the data that we have over to the cloud, to some manufacturer, someone in China for example. They process that data and then sends it back to the home. But no sort happens inside that cloud or if that data is shared with third parties. So, the cloud while they help in a way that reducing the cost of the devices because you don't need to have onboard storage and processing and sophisticated software onside the device. It is at the stake of user privacy. So, what is happening inside these clouds. So that is one thing, cloud might be very risky in a way. And you mention artificial intelligence, that is a big thing, but I don't know. All type of AI we are talking about.
54	E2	But what type, for example, a couple of months ago there was this self-driving car. It is a Uber in US, I am not sure if you have read about that. But that is one of the AI self-driving car when it kind of killed a person. So, that is also related to security, right so.
55	E3	What if you hack an AI machine? What happens than and especially if it is replicable like self-driving cars. If you have the whole system from above and you spread malicious attacks towards all the cars that are on the road right now. Is it one case, isolated case, where the woman was hit and she wasn't noticed or is it multiple cases happening at the same time. So, imagine combining AI, cloud and what happens at the same time if you start listing all these areas together and prioritizing and combining. What is happening.
56	E2	But also, you can create an AI algorithm or AI let's say that will be a hacker.
57	E3	Exactly.
58	E2	The AI is the hacker, automatic kind of hacking, more or less. But that might be also possible.
59	E3	AI fighting

60	E2	But even that might be. I read an article about how we as a society, are we ready for AI? I personally think that we are not because for multiple reasons. Technology has evolved so fast that we cannot trust the voice over interaction of that device, we still do not trust that. Right, because we said no, I am not getting accurate data and you don’t trust that. So, the trust is important also like how the simple user trusts those devices. That also affect sort of those things. And based on this article regarding AI it is one more thing that we are not ready, still behind these AI systems there is a lot of huge employment today of data scientists. So, what they do, they sort of massage this algorithm for AI because still they cannot make good decisions so that is why there is a lot of employment of data scientist when they are working behind these smart applications which they are not smart. To kind of do some work on them. So, still there is human and where there is human then there is a lot of security risks. Right, I can just access the data from as you say from the voice over Amazon echo and then I can just share this with my wife and say “haha can you see what they are doing right now”, somebody was fighting or whatever. The device constantly listens to you.
61	AS	What will you say like the, we have talked about the consequences, with the car and also with the cameras. Do you have another example of consequences with cyberattacks to smart cities?
62	E1	Yes, I think integrity is a very big issue with internet of things in general integrity, modification of data and that can happen in many cases. For example, imagine someone have assisted living, having medication at home and then you change the data, so I am sending my data to my healthcare provider and then suddenly someone change the data, imagine the consequences of that. That can be death possible death. But also, like changing a lot of data. Because Smart city evolves and smart cars in the end of the day. Imagine cars services. And then you change the data, you change the speed of the car for example. Or you break the distance automatically or you because the car has becoming a moving information system. What if the data the car download from the internet gets change, how will the car behave? Integrity is a very big issue with smart city in general and in internet of things. I would say I would give it the highest and then with privacy. Because in Smart Cities we are becoming like surveillance, like a society being survey all the time and this is a big topic. Do you have free choice if someone is always monitoring your daily lives, your daily habits.
63	E2	And someone is already watching us. Google for example.
64	E3	Actual the three of us have stated, given a statement together in a paper security has become a strength but ethics an expense of privacy. Literally there is no privacy and that is why we are moving towards this topic if you remember I mentioned her, I think. Where do you live right now as if there is a tower that watches you constantly, there is no privacy. Simply be connected, all of us.
65	E2	Ordinary, Google knows where is your home, where is your work, where your wife work or partner, where your kids go to school, where do you shop, when are you going to travel because you bought a ticket, all the

		routes, where you travel usually, how many transactions you are making so what will happens to those kind of data? This is very scary.
66	E1	And all your problems, because you search for them. And combine that with AI, because that can-do predictions. E2: By predictions I mean you can see that we can get a lot of suggestion because they know you go frequently, for example to Copenhagen ten times.
67	AS	But how do you think the citizens will be affected by this? Will they still want to participate in the smart city, or can it affect them?
68	E1	Your choice.
69	E2	It's like, a lot of people they use Facebook, I mean they use it because everybody uses it and is a part of it. We use it. It is very hard to not use the technology.
70	E3	You opt out.
71	E2	It is very hard.
72	E1	How do you opt out for a car to collect your data. You cannot, there is now. But I think, for example for the smart home most of them are no longer supply about the washing machine without having connection. It is a little bit hard to go back in time to not be connected. Even from the manufacturing point of view there is no easy option to do it. You have to get the device.
73	E2	So, everything will be connected. Pretty soon, even the refrigerator, so imagine you not get a good milk, if somebody hacks you.
74	E3	Just to add to that from an ethical point of view. Citizens can’t always choose what they want, so if a smart city concept is coming and it is evolving so rapidly, so it is covering so many areas that is what is going to happen. One of the simplest ways to see how smart city has evolved is to look at transport in particular, train stations, train metros, many of them are sort of AI, operating on their own and punctuality have increased since AI have coming in place and run these trains. And for people this is, if there is an exact every three minute metro at the rush hour, I appreciate that I don't even discuss if there is any privacy risks relating to me entering or bordering these specific trains when I peep or check in that I will be bordered that metro or train. Nobody is discussing that. But all of my data is recorded that I entered, at 13.37 my metro from Copenhagen airport train station to Copenhagen central. And someone hacking can know it when I have boarded, when I will be off that metro as well. And if I am a political figure that could be a very risky business in an American context for instance, maybe not in Europe or Scandinavia where politicians riding her bicycle and in other countries politician walking down the street with ten guards. If you have seen the north Korean leader with the runners after.
75	E2	He is in the car.

76	E3	He is in the car and the guards are running after him. That is the most extreme case in the world right now, but you just think about a useful citizen if someone will be traced for other reasons. It is very recent case, with this person I think she was from BBC, a reporter, she was kind of tralled and then also bullied and followed by a specific random person and was going to even kill her if she was not going out with him. It was like that. How much will these risks become if hackers have other intentions. Not one but one to many. What happens then?
77	E2	It is not only about hackers; it is about we took this example of accepting information from an ordinary camera. We know there are these lately a lot of fragmented of society based on the different beliefs about religions, and an ordinary guy could just go and see and then make some intentions, and then killing people.
78	E3	Just what happen in New Zealand just recently.
79	E2	Yes, he was streaming for examples alive his killings.
80	R3	So now this smart environment should actually have done the opposite, if it was smart enough it should have prevented these actions to happen instead of broadcasting it.
81	E2	That is what I said we are not ready, as a society but technology is also not ready. We say AI but I don't see it. And there are huge issues in security and not everybody thinks about it. Users are not aware and, in the end, it is the users that suffers the most. When I say users, I mean people, humans, ordinary.
82	E1	Yeah, don't think about AI because it is so scary in a way. Because in the end of the day you want to have choice, you want to have freedom in your life, we have control of information, but what if this information asymmetry. So, I have very little information that I can control. But someone, let's say the company providing the AI they have all that information about me, past information, with these algorithms you can predict but you not only predict you can also awareness me about, what I choose, like cases. But it is not AI, for example adjusting the Google search results, because we just leave first page of Google but do, we really have to trust the first page, there is even more pages inside Google. But how does the ranking algorithm work when they use AI. What is the choices that we have become something like that. An algorithm is changing our exceptions. Because with AI we have no choice. Maybe there is no human in the loop. There should be a human in the loop because the system should be for us.
83	AS	I think it was interesting what you say that we don't go to the last page, do we even choose by ourselves of do they choose for us. It is scary.
84	E2	That is for sure, we don't choose it.

85	AS	How do you think the security issues will continue when the smart city is more implemented?
86	E1	It is difficult to make predictions but with internet of things it seems like we have stepped more back than we had before. The internet has started. Because we have constrained devices, devices seem to be open, the internet manufacturers. A smart city will automatically inherit these advantages as well because smart city will use internet of things, how it will be, it will probably be worse at least at first, and then you start think about. Everyone knows security starts from the beginning. But it is always enough.
87	E2	Nobody starts with security thinking in mind first.
89	E1	Probably there will be new problems. Problems, which we have never faced before. Especially if you put the AI smartness perspective in it like new security problems. It is still like, I would say a spin of the previous problems, confidentiality, integrity, availability those kinds of problems but they will take a different turn I would aspect if you add the smartness to them. But the consequences can be more grave for example if you take for example when we talk about cookies and stuff when you are browsing the internet. The user has a choice because with computer you say down ... what is you put these devices that are constantly monitoring you, imagine this inside your home, now you go back, now you go outside, all the time surveillance basically. It will become good maybe for the government or for some companies who will monetize your information or may in some way predict crime, because that will help because you will get information. But then I as a normal citizen will i have the rights to reclaim my data, to change it, I don't think it is possible. And check what China is doing, they have these credits, citizen credits system or something like that. Where you get the benefits by how much you participate on Facebook, what your credit score, then you have no choice.
90	E2	Then you have to use the technology.
91	E3	If I know it well it is like how do you behave. In the society based on how you behave online so they can score you like a good behave citizen or badly behave citizen by tracking you what you do. And every single thing you do in China is tracked. Then you know for sure, any search, any post, any lie. Versus here a future employee might look at your LinkedIn profile or Facebook profile by asking for a specific by accept by paying for that, for that particular reason. but not that you are tracked for every single like, search, anything you have done, as soon as you enter your scored. Good citizen, bad citizen.
92	E2	And now they can verify it like physically as well.
93	E3	And the scoring has to do with the type search itself and if it harms China in any way, if you ask for Tirana square, in Beijing it was when they killed a number of students in a protest with tanks, that is forbidden news in China sort of. So, if you actually searching for those things within China in your Chinese citizen, this is when you can get the scoring as a bad citizen. You can start get scores like that. If you are a citizen

		asking for facts now you are thinking in with century are we lining in really.
94	E2	But even in the US there was this case it was a writer was writing about killings, how to kill my wife. And then suddenly after one hour, FBI came in, he didn't know what happening. Based on his keywords, they identified him as a potential threat. So, we are being monitored constantly.
95	E3	And actually, the guy is a very famous serial killers' novel writer.
96	E2	So, you see there is a missing, they miss some contextual data, who is that person. Not everyone is a killer.
97	E3	Instead of identifying that, go identify the New Zealand shooter, right. And you are missing that identification when it was apparently. When the New Zealand guy came out you got a lot of data stating that you could have prevent it. It was a history you could change.
98	E2	It was a dangerous guy. No, he even said one day before I will be killing, and people were following him. So, nothing happened by the system then.
99	AS	From your experience what would you say that the smart city needs to do to prevent the security threats? Yeah, we discussed other different solutions, like technical, policy, legal and governance. The technical mentions more like firewalls, end-to-end encryption stuff like that. But Governance is more how from the beginning what you think about it.
100	E1	You need to have strategy, management, operational. You need to start from the top, strategy and then you have middle management someone implementing this technical. And then you have operational, day-to-day running of the systems. But then what kind of controls you need with attack, you need technical control, you need administrative controls.
101	E2	It is also hard to follow legal aspects, especially small companies. They never follow these legal aspects. But an ideal security would be to think as I said in the beginning to think from day one about security, by design, mechanisms, bodies, what to expect, what are the regulations, thinks like that. But I think that will ever happen.
102	AS	I think they mention somewhere that most people they don't know they are attacked in organizations.
103	E2	Yeah and we will not know.

104	AS	Regulations, there should be stricter penalties for companies that do not become what they invite.
105	E2 & E1	Compliance is key.
106	E1	The public should be aware, they should have some basic know of security, basic information, if I buy a device from internet. Ito make sure that I change the default passwords.
107	E2	It is sort of security education, it is not only for developers, but also for the users.
108	E3	The problem, you buy things by default, implicit here it says here is the username and password. And it is default producing these technologies sort of have a thinking by stating this is a default password, the citizen who is buying whatever their profession is should kind of have a knowledge that default means it should be changed. The problem is that the company who develops that has a expertise so high that they cannot think at the lowest level of how it could mean to run the device.
109	E2	Often over engineers' things and they think this is perfectly fine. They don't test it with an end user.
110	E3	This should be known by a doctor or nurse and have no interest than to use this for the things that it allows at a medium. Why should they know. They have another profession. Overengineering or overthinking.
111	E2	Just to make sure, it is not related to security that much but take an example of Microsoft word how many functionalities there is. And how many an ordinary people are using. I mean maximum six-seven functionalities. You save you format. There is a lot of functionalities. That have been implemented so it is the same.
112	E3	So, what the users can do, and what they are maybe supposed to do. They don't use that function at all. Security is one of the latest functions they will check on.
113	E2	So maybe we need to think of user awareness security mechanisms, to create user experience for security. Because this is things that are missing. Because we don't design security with users. Maybe this could be relevant.
114	E3	This could actually be very relevant thing to come as an output for your thesis. I know you will have much more interviews. The problem is not only the technology and how it is developed. The complete other end, the user but what we should do for them. An interesting outcome.
115	AS	Thank you so much!

Appendix 2: Interview 1

Job position: Program leader Smart and connected city
Located in: Stockholm
Date: 2019-04-16
Duration: 32 min
Language: Swedish
Type of interview: Skype voice call

R1: Respondent 1
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	We found that Stockholm wants to be one of the worlds smartest cities by 2040 and therefore it should be very interesting to hear how you work with that? *Hej! Vi hittade att Stockholm ville bli en av världens smartaste städer år 2040 och tyckte därför det skulle vara väldigt spännande att höra om hur ni arbetar med det?*
2	R1	Yes, and if we are done before 2040 we are very happy as well. *Ja om vi är klara innan 2040 är vi jätteglada också.*
3	AS	Yes okay. *Ja okej.*
4	R1	But we have just started the work so that is something you should mention in the thesis that we have just started the work to be a smart city. *Men vi har precis påbörjat arbetet, så det är något ni ska betona i uppsatsen att vi har påbörjat arbetet med att realisera en smart stad.*
5	AS	Ah so you are just in the introduction now? *Ah, så ni är i inledningen just nu?*
6	R1	Yes exactly. *Ja precis.*
7	AS	I thought we could start with, is it okay for you that we record the interview? *Jag tänkte att vi kunde börja med, är det okej för dig att vi spelar in intervjun?*
8	R1	It is completely okay. *Ja det är helt okej.*
9	AS	Good! And do you want to be anonymous in the study? *Vad bra! Vill du vara anonym i vår studie?*

10	R1	No, it is not necessary. *Nej det behövs inte.*
11	AS	Okay yes so good. *Okej ja vad bra.*
12	R1	It would be fun if you want to send it to me when you are done. Det hade varit kul när det är klart om ni vill skicka den till mig.
13	AS	Yes, absolutely we will do that. And then we thought if would you like to tell a little bit about yourself and what you work with in the Smart City? *Ja absolut det ska vi göra. Sen tänkte vi om du ville berätta lite om dig själv och vad du jobbar med inom den smarta staden?*
14	R1	Mm, as you might have read so the council in Stockholm town (kommunfullmäktige) adopted a strategy for two years ago in April 2017 a strategy about develop the smart and connected city and 6 months later a program was created to drive this work and in that program I am the programleader. Connected to or in that program there are five projects. Two of the projects are called prerequisite projects (förutsättningsprojekt). Prerequisite to be able to be a Smart City. One of the projects is about to get an IoT platform and the other prerequisite project is about how we can handle open and shared data. *Mm, som ni har läst kanske så antog kommunfullmäktige i Stockholm stad en strategi för två år sen, april 2017, en strategi om att utveckla den smarta och uppkopplade staden och ett halvår senare så tillsatte man ett program för att driva det här arbetet och i det programmet så är jag programledare. Kopplat till eller i programmet så finns det fem stycken projekt. Två stycken projekt är så kallade förutsättningsprojekt, förutsättningar för att överhuvudtaget ska ha ska kunna ha en smart stad. Och det ena handlar om att skaffa en IoT plattform och den andra förutsättningsprojektet handlar om hur vi ska hantera öppna och delade data.*
15	AS	Okay. *Okej.*
16	R1	Open data is such that we can handle for anybody. Thus, open outside the city. And when we talk about shared data it is between different administrations (förvaltningar) and companies in Stockholm city. *Öppnade data är sånt som vi skulle kunna hantera för vem som helst. Alltså öppet utanför staden. Och när man pratar om delad data så är det mellan olika förvaltningar och bolag i Stockholm stad.*
17	AS	Okay. *Okej.*
18	R1	We have also connected three activity projects (verksamhetsprojekt) to this. One of them is about smart and connected lightening, another is about traffic control (trafikstyrning) and one is about smart locks. *Vi har också kopplat tre stycken verksamhetsprojekt till det här. Det ena handlar om smart och uppkopplad belysning, ett handlar om smart trafikstyrning, och ett handlar om smarta lås.*

19	AS	Okay. *Okej.*
20	R1	As soon as we have this technology, we will start to test what we call smart solutions. There is where we are today. We are purchasing an IoT platform, we are purchasing a system for smart lightening. And we are purchasing so called multifunctionsensors for the smart traffic control. Are you aware about what multifunctionsensors are? *Så fort vi har den här tekniken på plats så ska vi kunna börja testa det vi kallar för smarta lösningar. Så där står vi idag. Vi håller på att upphandla en IoT plattform, vi håller på att upphandla styrsystem för smarta belysningen. Och vi håller på att upphandla så kallade multifunktionssensorer för den smarta trafikstyrningen. Är ni medvetna om vad multifunktionssensorer är?*
21	AS	Maybe not really. *Inte helt kanske.*
22	R1	In our case when we talk about it right now it is a camera that can register traffic and in that camera, we can see pedestrians, public transportation, private cars, busses, and cyclist and so on. We can see from what way they come and what speed they have. But in our smart city we are not interested of that video that this camera can record, instead we are interested about this information that this camera gives. This is information about cyclists, busses, what speed they have and in what way they go. And from that information we can create a new traffic control in Stockholm. *I vårt läge när vi pratar om det just nu, så är det en kamera som kan registrera trafik, och i den kamera kan vi se gångtrafikanter, kollektivtrafik, personbilar, bussar, cyklister och så vidare, från vilket håll dem kommer, vilken hastighet de har. Men i vår smarta stad så är vi inte intresserad av den film som den här videon eller kameran kan spela upp utan vi är intresserade av den informationen som det här ger alltså cyklister, buss, vilken hastighet de har, vilket håll de åker till. Och utifrån det kan vi skapa en ny trafikstyrning i Stockholm.*
23	AS	So interesting. *Vad spännande.*
24	R1	So, there I understand we have touched security questions. *Så där har vid då tangerat mer säkerhetsfrågor förstår jag.*
25	AS	It sounds very interesting. First of all, I would like to ask you how you define a smart city? *Det låter jättespännande. Först skulle jag också vilja fråga hur du definierar en smart stad?*
26	R1	Stockholm have chosen their own definition of a smart city. We have said that it should make the life easier and increase the life quality for our citizens and visitors and we will also have the best company climate for companies. So, it is the people who live and are in the city when we talk about the smart city. It is not about the infrastructure as it might do in many other cities.

		Stockholm har valt en egen definition av en smart stad. Vi har sagt att det ska göra livet enklare, det ska höja livskvaliteten för medborgare och besökare och så ska vi ha det bästa företagsklimatet för företagare, så det är dem som lever och verkar i staden när vi pratar om den smarta staden. Det handlar inte om infrastruktur som kanske många andra städer gör.
27	AS	Okay so if we talk a little bit more about security. What challenges and problems with security do you see in all these initiatives you have in Stockholm? *Okej, om vi ska gå in lite mer på säkerhet. Vad ser ni för utmaningar och problem med säkerhet i alla de här initiativen ni har i Stockholm?*
28	R1	We have seen that there are all the time challenges when it comes to security from different ways. For the first, it must be secure information because all the data we have about our citizens. We can not tell, here is Olle Andersson bicycling. All this information that we collected should be anonymized. We are not interested of the video information we want to see what streams we have. We also have this IT-security that is very important that we must handle so no one can hack our system. And then when we implement new sensors, we need to handle so they do not fall down in the citizens heads. So, there are different kind of security we need to handle. And we do that of course. *Vi har sett att det hela tiden finns utmaningar när det gäller säkerheten från olika håll då. För det första är att vi måste ha en säker information för att all data som rör våra medborgare, vi kan inte tala om att här är Olle Andersson ute och cyklar. Utan all den typen av information som vi kan ta till ska vara anonymiserad, vi inte intresserad av videoinformation utan vi vill jobba och se vad vi har för flöden i det här sen har vi då den IT-säkerheten som vi också behöver hantera så att ingen kan hacka sig in i våra system som också är väldigt viktig. Och sen att när vi sätter upp nya sensorer så får de inte ramla ner i huvudet på folk så det finns olika typer av säkerhet som vi måste hantera i det här läget. Det gör vi såklart.*
29	AS	How do you make sure that the information become anonymous? *Hur ser ni till då att informationen blir anonym?*
30	R1	It is especially through information-classify this information and always follow up so we do it right. That right people have access to our systems and that we handle our services in that way that is decided based from the classing of information that have been made. So, all our systems and sensors need to information-class in this process. And that have we done to make it really easy for us, employed a security-coordinator to us so we have one person that dedicated, it is not just one person it is a company that will help us to do the right things when it comes to security-questions all the time. *Det är framförallt genom att vi säkerställer det genom att informationsklassa den här informationen och följa upp det hela tiden så att vi gör rätt, att rätt människor har behörighet till våra system och att vi hantera våra tjänster på det sättet som är bestämt utifrån den informationsklassningen som har gjorts så alla våra system och sensorer måste informationsklassas i den här processen. Och den har vi också för att göra det rätt så har vi knutit en säkerhetssamordnare till oss så vi har en person som är dedikerad, ah*

		inte bara en person utan ett företag som ska hjälpa oss att göra rätt när det gäller säkerhetsfrågorna hela tiden.
31	AS	Okay, are these persons involved in the projects then? *Okej, är de personerna involverade i projekten då?*
32	R1	Yes, they are all the time. These persons started for a few weeks ago and it was about that they had to sit down and resonate with the projects about what challenges they had and help them to see what things they could find that we had not thought about yet. So that we make the right things for our purchases. *Ja de blir det hela tiden så att vi, så att de här personerna började för någon vecka sen bara och då handlade det om att dem skulle sätta sig och resonera med projekten vad de har för utmaningar och hjälpa de att se vad finns det för saker de kan hitta som de inte hunnit tänka på ännu. Så att vi gör rätt saker inför våra upphandlingar.*
33	AS	Okay so good. Have you had any attacks against your systems today? *Okej vad bra. Har ni haft några attacker mot era system idag?*
34	R1	No because we don't have any smart systems implemented yet. But we have had attacks in Stockholm city, but I am not so involved in that work, but I know it has been. *Det har vi haft, inte mot några Smarta tjänster eftersom vi inte har några smarta tjänster ännu så har vi haft attack mot system i Stockholms stad, jag är inte så jätte involverad i det arbetet men jag vet att det har varit.*
35	A	Ah alright, how could you stop these? *Ah okej, hur lyckades de attackerna stoppas?*
36	R1	Yes, it is that we very early get the information that something is happening and then we need to handle that together with our suppliers. It is very little Stockholm do by themselves, we have outsourced the most of our IT. The suppliers have to handle this as fast as possible. *Ja det är att vi väldigt tidigt får reda på att det hänt saker och sen så får vi hantera det här tillsammans med våra leverantörer. Det är väldigt lite saker som Stockholm driver själva, utan vi har outsourcat det mesta av vår IT. De leverantörerna som får lösa det här så snart som möjligt.*
37	AS	How do you think the attacks will change when more Smart City systems are implemented? *Hur tror du att attackerna kommer förändras sen när fler Smart City systems är implementerade?*
37.1	R1	Oh, it is a little philosophy question, I do not know actually, we always need to be secure and try as fast as possible to identify an attack and let us say, when data is used in the wrong way. In ways that we might not even could think about that it was possible. If we do that, we need to shut down that delivery of information or data so it is not possible to use that in wrong ways. The most important is that we as early as possible get information when something is happening. It is possible that it will happen and that there are things that we actually have not thought about as we must be able to solve very fast when something happens.

		Oj, det är lite filosofiskt fråga, jag vet faktiskt inte, vi måste hela tiden vara säkra på och försöka så fort vi kan identifiera att en attack eller en låt oss säga, data används på fel sätt. Sätt som vi kanske inte ens skulle kunna tänka oss att man skulle kunna göra. Att om vi gör det så ska vi kunna stänga ner den leveransen av information eller data så att man inte kan använda den på ett felaktigt sätt. Det viktigaste är att vi får så tidigt som möjligt får information när något håller på att gå snett. Det är säkert så att det kommer att hända att det finns saker som vi faktiskt inte har tänkt på som vi måste kunna lösa väldigt snabbt på plats om det händer något.
38	AS	What would you say are the biggest risks that could happen to the city and the citizens? *Vad skulle du säga är de största riskerna som skulle kunna hända mot staden och de som lever i staden?*
39	R1	Today we do not see any big issues like that. It is about remake the services. If we think about the traffic control today, we use sensors today that monitor our traffic it is just that these sensors are in the ground. And when a car drive over them, they notice that now a car came here. But the sensor can not feel if there is a bus or a bicycle or a private car. Instead we try to get these sensors in cameras instead which makes it better for us to control the traffic. So it is the control. Then the next step is to share this information as open data. So that other actors can use this data and maybe create a new traffic service that use this data we deliver an in absolute cases of that traffic services would not work so good. That is at least what I can think about today. I have hard to imagine that we could get a system where someone could hack our traffic systems and shut down all traffic system. I assume that we have such security that it is not possible. Instead it is about that if you deliver data to one place and another data to another place and you could might combine this data in a way we had not thought about... That is something we talk a lot about sometimes. When two or three data sources tell something that we could not even imagine was possible. Do you understand what I mean? *I dagsläget ser vi inga såna stora risker. Det här handlar om att göra om de tjänsterna. Om vi tänker oss trafikstyrningen idag så använder vi ju sensorer i dagsläget när vi styr vår trafik det är bara det att de här sensorerna är nergrävda i marken. Och när bilar kommer över dem så märker dem att aha nu kom det en bil här. Men den kan inte känna efter om det är en buss eller en cykel eller en personbil. Istället så försöker vi få in de här sensorerna i kameror istället som då ges på ett bättre sätt får oss att styra trafiken. Så det är liksom själva styrningen. Sen i nästa steg är då att vi delar all den här informationen som öppen data. Så att andra aktörer kan använda sig av den här datan, kanske bygga en ny tjänst en trafiktjänst som använder utifrån den data som vi levererar. I absolut värsta fall om den trafiktjänsten inte skulle kunna fungera bra. Det är i alla fall så vad jag skulle kunna tänka idag. Jag har svårt att tänka mig att vi skulle få ett system där någon skulle kunna hacka sig in i våra trafiksystem och släcka ner alla trafikljus. Det förutsätter jag att vi har en sån säkerhet att det inte är möjligt. Utan det handlar snarare om att om man levererar data på ett ställe och en annan data på ett annat ställe och man kanske kan kombinera data på ett sätt vi inte kunnat tänka det är nog det vi mycket pratar om ibland. Att när två eller tre datakällor berättar någonting som vi inte ens kunde tänka oss att det var möjligt. Förstår du vad jag menar?*

40	AS	Yes okay. How do you think about privacy in combination with security? *Ja okej. Hur tänker ni gällande privacy i kombination med säkerhet?*
41	R1	I do not really understand the question. *Jag förstår inte riktigt frågan.*
42	AS	Okay but what information is the most sensitive that is stored in the system? *Nä men vilken är den mest känsliga informationen som samlas i systemen?*
43	R1	Today it is, what we can see today is just when someone has passed or someone have walked by, we can see if a light is broken that is what we talk about in two of our systems today. The system that we talk about is the one with smart locks. There we could see today in homecare that we have a service for the locks. And there a home cares have the right to visit your mother or dad at sometimes to help them. It is very important with the security of these so that not anyone else could enter at these times. The information about that we have not started to discuss. But maybe you could see that someone have been at my data during the day from the homecare for example. And there we need to handle the security in a good way. *I dagsläget är det, det vi ser just nu är bara att någon har passerat eller någon har gått förbi, vi kan se att en lampa är trasig det är det vi pratar om i två av våra system idag. Det systemet som däremot som vi pratar om det är det här med smarta lås. Där ser vi idag inom hemtjänsten vill ha en låstjänst där en hemsjukvårdare har rättighet att komma in hos din mamma eller pappa vissa tider för att hjälpa dem. Då är det väldigt viktigt med säkerheten där så att inte någon annan person kommer in under de tiderna. Själva informationen om det där har vi inte liksom börjat diskutera. Man kanske skulle kunna använda nu ser vi att någon har varit hemma hos min pappa under dagen från hemsjukvården till exempel. Och där behöver vi hantera säkerheten på ett väldigt bra sätt.*
44	AS	Yes. *Ja.*
45	R1	And then it is important with privacy as you said. There are services in other municipalities that I know they use today. For example, that they implement night cameras at elderly people that need help and then they can log in and see with help of these cameras and see if the person sleeps or if the person have fallen from the bed or fallen when the person visited the toilet. It is a kind of support for them, but it is in the same do you really want this and that must be handled together with these persons. But our challenge with the smart city is to use technology so that everyone can stay at their home a little longer than be forced to live at one home cares. *Och då är det viktigt med privacy som du säger. Det finns ju tjänster i andra kommuner som jag vet att man använder idag. Till exempel det här med att man sätter upp nattkameror hos äldre personer som behöver hjälp och då kan man gå in och titta med hjälp av de här kamerorna och se sover den här personen eller har den ramlat ur sängen eller har den ramlat när om den varit uppe på toaletten. Så det är ett stöd för dem men det är samtidigt vill man verkligen ha det och det måste man då hantera tillsammans med de här personerna. men hela våran utmaning med den smarta staden*

		är att få att använda oss av teknik för att vi i bästa fall kan bo kvar hemma lite längre än tvingas bo på ett äldreboende.
46	AS	If you then think about this with privacy, if it was a security problem that would lead to that sensitive information became public. How do you think the citizens in the city would be affected by this? *Om man då tänker det här med privacy tror du om det skulle vara ett säkerhetsproblem som skulle leda till att känslig information läcks ut. Hur tror du att invånarna i staden skulle påverkas av det?*
47	R1	Of course, in a bad way. That is exactly what just happened when the service 1177 showed that it was possible to see what some people had told about their diseases and that was nothing that they were happy over that had been possible. So today I do not believe that it would be a very big problem but if it would be very many things like this that happen then it would of course lead to that people become skeptical and the big issue is that people do not dare to be public and honest and that is an even bigger problem. Because for example in the healthcare, if we do not talk about how we feel we will not get the right treatment. *Självklart negativt det är ju precis det som hände nyligen när den här 1177 tjänsten där visade sig att man kunde höra människor som hade berättat om sina sjukdomar så var ju ingenting som man var speciellt glada över att höra att det hade varit möjligt. Så att i dagsläget så tror jag inte att det skulle vara ett jättestort problem men om det skulle bli väldigt många sådana här saker som händer då blir det självklart att man kommer vara skeptisk och den stora risken är väl att människor inte törs att vara öppna och ärliga och det är nog ett ännu större problem till exempel i sjukvården för att talar vi inte om hur vi mår, får vi nog inte rätt vård.*
48	AS	No exactly and that could affect the healthcare in a bad way? *Nä precis, och det skulle kunna påverka sjukvården väldigt negativt.*
49	R1	Yes exactly. *Ja precis.*
50	AS	Is there any other area that could be affected in a bad way of this? *Är det något annat område som skulle kunna påverkas negativt av detta?*
51	R1	I have not reflected over this. But these kind of questions we always need to bring and in all the projects that are performed you have to think about what can the risks be with this from different aspects. That is probably the most important we take with us. That you cannot leave these questions to an expert. Instead you have to work together with the experts to get help and be able to solve this in a good way. *Jag har inte reflekterat riktigt över detta. Men de här frågorna måste vi ha med oss hela tiden och alla de projekt som genomförs så måste man tänka vad kan det finnas för risker med det här ur flera olika aspekter. Det är nog det viktigaste vi tar med oss. Att man inte får lämna de här frågorna till en expert utan man måste jobba tillsammans med experter för att få hjälp och kunna lösa det här på ett väldigt bra sätt.*
52	AS	Yes, we have talked a little bit about it, how you work to prevent all these issues that you use a person that is responsible for security.

		Ja vi har varit inne lite på det här hur ni arbetar för att motverka alla de här riskerna, att ni har en person som är ansvarig för säkerheten.
53	R1	Yes, it is a company with many persons. *Ja det är ett företag med flera personer.*
54	AS	Mm okay and they are involved in the project? *Mm okej, och dem är med i projektet?*
55	R1	Yes. *Ja.*
56	AS	Do you have clear goals in the project from the beginning when it comes to security? *Har ni tydliga mål i projektet redan från början när det gäller säkerhet?*
57	R1	No, we have not any goals when it comes to security, it is something obvious. It is a part of all our projects that in a secure way be able to handle the systems in Stockholm city. *Nä vi har inga mål när det gäller säkerhet utan det är en självklarhet. Det finns liksom i bisats i alla våra meningar att på ett säkert sätt ska man kunna hantera systemen i Stockholm stad.*
58	AS	How is it when it comes to policies and regulations? *Hur tänker ni när det kommer till policy eller regulationer?*
59	R1	That is something we need to handle during the project. Today it is important that when we start with a work with these three projects we have or the five project I could say. Start with identify what aspects we see as general for all projects we need to formulate regulations that should be for the entire city. It can be policies as well, this is how you should do to be allowed to implement a sensor and share the information. That is also a part of the smart city, when we talk about the smart city Stockholm that we need to work broadly. Every department should not create the wheel. Instead we should work broadly in the entire city and we should collaborate between the different departments and companies. *Det är sådant vi måste lösa under resans gång, vi resonerade idag senast det är viktigt när vi börjar ett arbete med de här tre projekten vi har eller fem projekt ska jag säga. Börja vi identifiera aspekter som vi ser är generella för samtliga projekt måste vi se till att vi formulera sådana riktlinjer eller anvisningar eller vad man nu kallar dem som ska då gälla för hela staden. Det kan vara policy också, så ska man göra för att få sätta upp en sensor och dela information. Det är också lite av den smarta staden, när vi pratar om den smarta staden i Stockholm att vi måste jobba brett. Varje förvaltning ska inte uppfinna hjulet själva utan vi ska jobba brett i hela staden och så ska vi samverka mellan de olika förvaltningarna och bolagen.*
60	AS	Yes okay, I thought about when it comes to education and training from a security perspective do you have that? *Ja okej, jag tänker när det gäller utbildning och träning för de anställda från säkerhetsperspektivet har ni någonting sånt?*
61	R1	Because we have not started anything yet, we have not either started that but that is obvious and important. We have GDPR and that is something all

		employees should have learned and be able to handle. And that is an important aspect in this. At the same time there are many more and the security questions become more important so we will probably work with that when we implement these sensors. But this is as important no matter in what service we have in the city, so it is not something special for the smart city, it is important in the other cases and services we have. *Eftersom vi inte påbörjat något ännu har vi inte påbörjat det men det är självklart och viktigt. Vi har ju GDPR som samtliga anställda ska ha gått igenom och kunna hantera. Och det är en viktig aspekt i det här. Samtidigt så är det många fler och säkerhetsfrågorna blir viktigare och viktigare så att det kommer vi säkert arbeta med så väl när vi börjar sätta upp de här sensorerna. Men de är ju lika viktiga oavsett i vilka tjänster vi har i staden så det är inte unikt för smarta städer utan det är viktigt i de andra fallen i andra tjänster som vi har.*
62	AS	I think we talked a little bit about this that the technology need to work in a secure way. Do you have any special ways to work with this? *Jag tror vi pratade lite om det att tekniken måste fungera från ett säkert perspektiv, har ni några speciella sätt ni arbetar med där?*
63	R1	We will probably have that, but it is not important if it is enough, I do not know that. Then it is a lot about to reduce the ones that have the rights to log in to our systems. So, there are many different aspects. The ones that works with attacks is often one step before, so it is important to follow the market and make sure that the services we have are as secure as possible against attacks. *Det kommer vi säkert ha, sen om de kommer att räcka det vet jag inte. Sen handlar det väldigt mycket om att minska de som har en rättighet att gå in i våra system. Så det är många olika aspekter. De som jobbar med attacker är ofta steget före så det handlar om att följa den marknaden och se till att vi har tjänster som så gått det går är säkrade för attacker.*
64	AS	How do Stockholm think when they purchase different systems from suppliers, do they make sure that these are secure in any way? *Hur tänker Stockholm när de köper in olika system från leverantörer, säkerhets kollas dessa på något sätt?*
65	R1	Yes, as it is now as I mentioned we are working with some purchases and then this security company is involved in them and they will go through these purchases to make sure that we have thought as far as we can. At the risks that could be. *Ja nu har vi som jag nämnde då så håller vi på med ett antal upphandlingar och då är det här säkerhetsföretaget inblandat i dem och dem kommer gå igenom dem upphandlingarna för att säkerställa att vi har tänkt så långt vi kan. På de risker som kan finnas.*
66	AS	Ah that sounds good, what would you say are the most important ways for the security in the city? *Ah det låter ju bra, vilka skulle du säga är de viktigaste sätten ni arbetar med för att säkra säkerheten i staden.*
67	R1	Yes, the most important is that we always have it in mind from all aspect. I think it is important that everyone that work in our projects thinks about

		these questions all the time and then that we collaborate with experts and ethical questions that are important. We have that in mind all the time, that is important. *Ja det viktigaste är att vi har det i åtanke hela tiden och att det är viktigt ur alla aspekter jag tror det är viktigt för alla som jobbar i våra projekt tänker på de frågeställningarna hela tiden och sen att vi också samverkar med experter folk som sitter med etiska frågeställningar som är viktiga. Vi har det i åtanke att ha det i åtanke hela tiden, det är viktigt.*
68	AS	Okay, I thought about when it comes to resources and time how much do you add on security? *Okej, Jag tänker när det gäller resurser och tid hur mycket läggs på just säkerhet?*
69	R1	First of all, have we a company that work with this in our program full time but do we need more will we look over it. It is nothing we can say that we do not have more money and we continue, instead we always need to develop our services with the highest security. *För det första har vi upphandlat en person eller ett företag på heltid för att hantera de här inom vårt program, men skulle det behövas mer måste vi se över det och se till. Det är ingenting man kan säga att nu tog pengarna slut utan då fortsätter vi utan vi måste hela tiden kunna utveckla våra tjänster med högsta möjliga säkerhet där det är befogat.*
70	AS	Okay, is it anything else you would like to add to make sure that the smart city is secure? *Okej, finns det något mer du vill tillägga som ni arbetar med för att se till att allting är säkert i staden?*
71	R1	No not right now, I think that we have these questions and that is what is most important. It is also, important that we try to see what happens on the market and see what are the risks because there might always come new risks that we have not looked at or not even thought about and that is our big challenge. *Nej inte just nu, jag tycker att vi har de här frågorna på agendan och det är det som är viktigt och det viktigaste är också att försöka hänga med och se vad finns det för risker för det kommer kanske hela tiden nya risker som vi inte har tittat på eller inte ens kan tänka på och det är dem som är vår stora utmaning.*
72	AS	Okay and how will you do this? *Okej och hur ska ni göra detta?*
73	R1	It is important to have jour with the rest of the world and understand what happen and have a view on the rest of the world all the time. *Det gäller att ha jour med omvärlden och förstå vad som händer och ha en omvärldsbevakning hela tiden.*
74	AS	Yes, you talked a little bit about that you share information between the departments in Stockholm, do you do that also between different cities in Sweden?

		Ja du pratade lite om att ni delar lite mellan de olika avdelningarna i Stockholm gör ni det även i Sverige mellan olika städer delar med sig av sin information.
75	R1	Information that we have said is okay to share is said that we will share. When we talk about the shared data it is information that we want to have secure in the city. The open data should we be able to share with everyone whenever and that data can we share with municipalities and companies. And that is might the most important that we can work on the same way when it comes to different municipalities that are close to each other so that we can develop new clients for each of them. It can be anything, let us say that we have a ride service for the people that ride. But the people that ride they do not look at the different municipalities instead they ride in different municipalities and then you want the service to work on the same way no matter where you are, so it is important and the next step is that municipalities start to collaborate and share data on the same way so it is possible to create services. *Information som vi sagt att vi får dela det är sagt att vi ska göra, när vi pratar om den delade data så är det information som vi vill ha säker inom staden. Den öppna datan ska vi kunna dela med vem som helst och den kan vi dela med kommuner eller företag. Och det är ju det viktigaste kanske att vi kan arbeta på samma sätt när det gäller olika kommuner som ligger nära varandra så att vi kan skapa nya tjänster för en, det kan vara vad som helst låt oss säga att vi har en ridtjänt för de som rider med de som rider tittar inte på kommungränserna utan de kanske rider över flera olika kommuner och då vill man att den tjänsten ska fungera på samma sätt oavsett var man befinner sig, så det där är viktigt och nästa steg är att kommuner börjar samarbeta och dela data på samma sätt så det är möjligt att bygga tjänster.*
76	AS	Is it anything else you want to add? *Ah okej, detta har varit jätteintressant att lyssna på, är det något mer ni vill tillägga?*
77	R1	No. *Nä.*
78	AS	Is it okay if we contact you if we have any other questions? *Är det okej om vi kontaktar dig om vi har några fler frågor?*
79	R1	Yes, you can do that. Good luck! *Det kan ni göra. Lycka till!*
80	AS	Thank you so much! *Tack så jättemycket!*

Appendix 3: Interview 2

Job position: Project leader for Smart public environments, Future by Lund
Located in: Lund
Date: 2019-04-18
Duration: 37 min
Language: English
Type of interview: Face-to-face

R2: Respondent 2
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text	Coding (Base nodes)
1	AS	So, we found your email address like on IoT Sweden and you had a project together with Malmö in like workplaces, smart workplaces. Can you tell us more about yourself and what you have done recently?	
2	R2	Yes, so I am working here at future by Lund, at the municipality and innovation office and I am the main project lead for the smart public spaces projects which is focusing around IoT and digitalization. Apart from that I am also driving an innovation projects regarding the digitalization in the city and the IT. I have only been in the, working for the municipality for the last 1,5 years. So, I have been at RISE before, which is the research institute in Sweden and before that 15 years in Telia where I worked with IoT innovation and business development.	
3	AS	So, you are a main project leader and that is your main responsibility in these projects?	
4	R2	Yes.	
5	AS	And what is a smart city according to you?	
6	R2	Well a smart city is kind of, it is a broad thing. It could mean almost anything, like all of this kind of things. But a smart city is basically about utilizing our resources in a better way. My focuses are of course to use the ability to digitalization to make. I mean, you can do smart cities in many ways. It could be about energy, efficiency and stuff like that, but my focus is to try to use the digitalization in different ways. If it is IT, when it comes to sensor and stuff like that to make sure that the city is smart in many ways. It could be to reduce waste of energy, it could be to make better life for the citizens, it could be many stuff, but my focus is the use the digitalization in order to make the city smarter.	

7	AS	Okay. So, what smart city initiatives do you have here in Lund?	
8	R2	Excuse me.	
9	AS	Smart city initiatives or projects do you have here in Lund?	
10	R2	Yes, I think we have quite a few. So, I have a couple that is focused regarding when it comes to IoT, and that is how to use different kind of sensors in the city to make sure that we get a smarter city. For instance, we connected bikes in the city for the cyclists to make sure how they run their bikes to make smarter decisions when you plan bikelanes, for instance. We have done, when it comes to collecting trash to make sure that we get better planning. We have done projects regarding measuring the, what do you call it, the moisturing the soil and the parks, how we can make smarter decisions when it comes to when you should actually water stuff. So, we have run several different kind of small projects to see what we could do, that kind of makes the city smarter in a whole. And then we have projects on a larger scale that is more about the kind of platforms and how we should be able to tie different streams, digital streams together. To be able to share data between different, it could be departments, it could be between the city, the municipality and the other actors in the city. To be able to share data between each others, to be able to make smarter decisions in the city. And we will also establish a test-bed in the city where we try to utilize the whole city as a test-bed for doing different kind of small test and try proof of concepts. So that is something we have built up as well. When we have spoke about having the own technology and how the process and stuff like that ready in the city, and then enabling that for all the actors in the city. Which includes citizens, students, SMEs, entrepreneurs, big companies, large companies and the municipality itself to be able to use the test-bed and take away basically all the things that can hinder you to try and play with the city and make sure that you find the right solutions.	
11	AS	Are these projects implemented in the city?	
12	R2	Excuse me.	
13	AS	Are the projects implemented in the city or will you implement them later?	

14	R2	The projects?	
15	AS	Yes.	
16	R2	So, the concepts we are running them inside the city, yes. So, we are trying to, I think most projects are, it is much better if you can try to run them in the right environment. It could have the right… I mean a lot of test-beds we have seen or basically they are put up in a building or kind of in a small place where you can have the test-bed but that usually don't give the right result. But if you can try to the right kind of environment, it is much better. We will have a result that much better reflects the kind of, the true situation having for roll-out. So, we are trying to use the whole city as the playground in that sense.	
17	AS	So, what are the security issues, like with these initiatives?	
18	R2	Yes, when it comes to digitalization, I mean there is several things that can go wrong. So, what you are trying to do is to work together with actors that are quite knowledge in the area when it comes to security. For instance, when it comes to smart public spaces, we have a, kind of a, there is a project on the side that is totally focused on security that is not runned by the municipality. It is actually runned by mobile heights and RISE which are the, RISE have a security lab in Lund. So, they, but they are using the things that we are building up, our test-bed as a ground for see how safe it is and what kind of measures we have to take to make sure that we kind of have a secure system. Then again, security can be many things of course. It depends on what you mean by security. I am talking about securing that no one can tample with the digital streams.	GMS
19	AS	Like, when we talk about security we are about cybersecurity and how you can prevent cyberattacks.	
20	R2	Yes, so this is about cybersecurity. So, for instance, we have a project where we are building out, we are connecting the kind of grey boxes you see around the city which is the electric cabinets, building up a nesh-metric between them. And for instance, if we have a non-secure network people are able to kind of tample with one of the nodes and you can insert data in that, and we can have a whole system. And that is one of the things they are focusing on in that project, to make sure that we have the right cybersecurity on top of that system. Because they, obviously in the municipality we don't have the expert knowledge in that area. But since we are bringing RISE in to table they have those experts. Trying to make sure that we can create a secure system as possible, sometimes if you imply to	GMS

		much security as well, we get a system that is not doing any good as well. So, it is kind of a trade-off.	
21	AS	So, like if anything happens what do you think this could lead to for the city and for the citizens? If it is like a cyberattack?	
22	R2	I think. One of the things is of course that you get distrust of the system, you don't have trust in the system. No one is going to trust the data that comes out of it and then it is basically useless. So, that is obviously something that we have to work with. Also, I don't know, it can probably be anything. If you are able to tample with the data you can probably make a lot of damage, if the data is used to control something else. If it is something important and if it is actually used to control a whole system that could be a fault of course.	CSP
23	AS	Have you had like any attacks, like cyberattacks for the projects or the systems that are smart?	
24	R2	No.	
25	AS	When you do the projects, do you identify what issues there are? Or how do you like manage that?	
26	R2	Yes, so as I said when it comes to the security in this aspect we have, we are not doing it in these projects. It is actually done in the other projects, they are looking on the architecture that we have built up and see what type of, kind of if there is any hole, any gap in that metric. And that project, they are running it as we speak so it is not finished. So, basically what the outcome we hope with that project is that they give us kind of a reference architecture of what kind of security measures we have to take when we build up this kind of metrics. Otherwise, I mean it is not like we are building a totally unsecure system today, we are not building the system by ourselves. We are working together with the industry actors and it is… so in this project we have something like 35 different actors in this place, like it is Sony, Ericsson, Telia, smaller platform providers like Sensative than all other players. And of course, they also work everyday with making sure that their systems are safe. So, it is not like we are trying to build up this system that control it all, but still when you put many puzzle-pieces together it could build kind of holes in that whole puzzle that could offer opportunities for someone to break in. So that is what they are trying to do in that security project, to make sure that they look into the whole architecture that there are no kind of link that you can break in the whole chain.	SC + TS + GMS

27	AS	What do you think are the biggest issues for the security in your system or projects?	
28	R2	I think, we take many parts and put it together, maybe in a fashion that we haven't done before. So, sometimes I think it is hard the whole implications of that so that is why you have to make sure that the whole chain is working together because piece by piece they probably are already tested and working well. But when you put them together, its kind of makes the whole system weak if there is only one weak link. And when we are starting to collect a lot of data, and we are trying to share the data between different actors as well, it is really important that we can rely on the data that we collect. And also, that we can rely on each other's as different actors that is going to share data between each other, otherwise the whole system will fall because nobody will trust each other, and we will not be able to use it. So, there is a lot of work on top of the… when you talk about the cloud platforms when you actually collect all the data and when you are able to set who is going to share data with different players. And that is place where we also have to make sure that you have the system that you can trust. And that you are able to mix, both data that is not being shared openly with data that is being pretty much open to share. So, that is a challenge to make sure that they have a system that can support that.	SC
29	AS	So, do you think the security can affect the privacy of the citizens?	
30	R2	Yes, of course it could do if we start to collect that type of data. We haven't been working with that type of data. I mean, of course, when it comes to when we measure how the bikes are moving around in the city it is obviously that we are measuring how the bikes are and if you just collect them totally open you could probably dig back and see who is doing what. So, in those kinds of projects they always have to take care of how they actually make sure that they, the data is not connected to one person or something like that. We have also done measurements together with Telia when it comes to how people are moving around in the city based on how the mobile phones are moving around. And in that sense, it is actually demo actors that are making sure that we are not able to connect to a user. Because obviously, if you go into their management system you can see which users. But they have this kind of, the system, there have to be at least 5 persons' doing exactly the same thing for us to be able to see that what is played out. That is one way of making sure that you can't break the integrity then if there is to few doing the exactly the same thing. It can start kind of having a pattern of or going down to one person and then you break	RC

		the privacy. So that is something your integrity, that is something you have to look into in every case.	
31	AS	So, how do you think about privacy in the smart city? It is a broad question.	
32	R2	As I said, for every kind of proof-of-concept or whatever project we are starting to do we have to think for what it means. Sometimes there are issues and sometimes there are not. When there are issues, we have to take cause of course. So, as you said, it is a broad question. It is hard to say exactly how, because it differs...for every kind of stuff we do. We have to take that into account.	
33	AS	How do you think privacy breaches can affect the smart city systems?	
34	R2	As I said from the beginning, this is definitely a game of trust. So, if you break the trust it is probably not going to run those kinds of… at least not those part that smart city projects that involves the citizens and their private data. So, you will have to take care of what you are doing before and not just… So, we, as I said, if you want to do those type of projects you will have to plan before you just go out and do stuff like that. And you will have to be able to communicate as well. Normally when you do those kinds of tests, it is not on a broad scale. So, you have maybe, in the bicycle test we had a couple of hundred people and you have to inform carefully and, of course, what could happen and so on. Involve the know of how we are handling the data and what could happen and so on. It is much easier to handle if you are open in the beginning, then trying to cover up in the end. So, and I also think these citizens are more willingly to share the open if you tell them what you are doing and what you are trying to achieve. And what the risks are and what could happen if something happens. The big risk is if you are just trying to do something and you collect data while people are saying "what are you doing?" and then you are doing something else. I think that if you build up trust, I also think that the citizens are more able to kind of cope with if you have some small stuff that is happening that you are not supposed to do. As long as you are actually telling them why it happened and so on. And what you are taking permission to make sure that it doesn't happen again. So, I think it is a lot about trust.	CSP + RPLS + GMS
35	A	So, like our focus with our thesis is about solutions and what smart cities are doing. So, if you could talk about what security solutions you have, because in some literature are mentioning like technical solutions, policy and regulatory and legal solutions. And also, governance and management solutions, and do you have like any solutions	

		here in Lund that you think about or you will implement in these projects?	
36	R2	Well, I mean… there is obviously a lot of security protocols lying in the project that I don't expert in and can't really give you insights on how they work when it comes to essence on how they are using the... As I said, we have this open test-bed that is basically free for anyone to use. We are also trying to use policies or agreements towards those who are using it. Because as we are not running it, I mean we are not charging you anything for using the networks. We also have… since we don't have any money coming in, we have tried to do this as simple as possible as well. So, we are also pushing over a lot of responsibilities towards the end-users. Saying basically that it is they that are using the network have to make sure that they don't break any laws or doing any stuff that they are not allowed to do. That could happen of course and if we discover we basically have to face the consequences towards that, but we are trying to push the responsibility out towards the users of the system. But when we are running the projects ourselves, we have to make sure that we try to take the... as serious as we can and as I said, we are working together with the industry actors in this field. So, we are not trying to do it by ourselves. And it differs, all the projects have different solutions, it is basically hard to just... But what we try to do when it comes to the cloud platforms, those things, we try to do it based on standards as well so we are trying to use standards that we are basically, same standards that we have in Europe. Something called like fire ware, for instance, to build up the system. And that is not only for the security, but it also gives us the ability to build the same systems as the other cities today with a shared digital twin. So, we take partnering activities, we are trying to kind of form a Swedish architecture for this as well. Then, obviously, security is important.	TS + RPLS + GMS
37	AS	You talked about this open test-beds, so you can use them to try that it is secure or how do that work?	
38	R2	Not to try that the system by itself is secure. Actually, it is focused around IoT and being able to make, that you can try different solutions so you can for instance put out sensors in the cities that references that on is, let's say you want to measure the air-quality. So, we are making sure that it is really, that the communication systems are already there, the cloud platforms are already there. So basically, what you have to do is deploy the different sensors that you want to use. And then you can collect the data in the other end of the cloud platform and also be able to share the data between other actors. So, you don't have to	

		build up the whole chain of, for instance, selecting the communications systems that we have Laura, we have "narrowed" IT, we have Bluetooth mesh. It is just a lot of different technologies for kind of sending zero and ones for their…	
39	AS	And I was thinking like also for in the beginning of the projects do you set goals for security and how you should work with security in the project and?	
40	R2	No, as I said, we haven't had that focus in our projects, so we are not setting goals. Basically, we are saying that we are using kind of industry standards when it comes to that and then it is the other project that is who is really focusing on the security issues. And if you want to talk to those guys, I will give you their contacts.	GMS
41	AS	Absolutely.	
42	R2	Because they are the ones that are experts on this and could answer this in-depth question regarding when it comes to cybersecurity questions.	
43	AS	Yes, that would be really good.	
44	R2	Yes, I think so.	
45	AS	I also have a question here like, but maybe that is also, maybe they can answer this better but like do you work with privacy by design and security by design in your projects? It is like if you implement security through the whole process.	
46	R2	Yeah, since we are not implementing ourselves it is actually our, the government that we work with who are implementing. Of course, we are talking about them to make sure that we have secure systems, but we are not the experts, we are not able to say exactly how secure they are. So that is what they are doing in the other project, looking through the whole chain and making sure it is a secure system and be able to have the architecture that we can then implement in the projects in the future. So, because we have not implemented a full-scale smart city kind of digital platform in Lund at the moment. We are still running test-beds, so it is kind of in a small kind of scale at the moment. But ones you want to enrol this out kind of in a big scale, almost like run an entire city on a smart city platform. Then you definitely have to make sure that you have all the security measures in, but we are not really there yet.	RPLS + FS

47	AS	So you decide what technologies that should be implemented in the city and the other project they like make sure it is secure or?	
48	R2	Yes, I mean what we are doing is basically that we are looking at different use-cases that we have challenges in. So, we are starting with the challenges that we have in the city and then from that we are trying to select both the right partners that bring in the right technology today to solve the solution in the best way. And then the other project on the side is going to work the test that we built up to see if there is any kind of hole in the whole security architecture.	
49	AS	So, they are just focusing on the security aspects?	
50	R2	Yes, they have a project that is just focusing on security and they are using our test-bed architecture as kind of their, their… they are using that as an example and that is really good for us, of course. But we have, they are running it now, so we don't have the result from it yet.	
51	AS	No. I was also thinking, if you implement security in your projects, what solutions do you think are mostly important, so it gets implemented right? Like the technical or governance or regulatory solutions?	
52	R2	I guess they all span different, probably answering different questions. I don't think one could kind of be replaced with the other one, so I think you have to probably look for the whole, all of three different areas and implement security in all those levels.	HS
53	AS	Do you have any technical solutions for make sure that you will not be attacked by cyberattacks?	
54	R2	Well, as I said, as we are using different actors and their technology. For instance, we are using the "narrow" and IoT, which are a technology from telecom rentors. Which basically, in this case is Telia and they of course, obviously have a lot of different measures for making sure that it is a safe network. So, we are not trying to step in there and say how they should do that. But, also we are trying new different type of technologies and they haven't been so much proven, like for instance building up the Bluetooth mesh network have nobody else done before. And that is why it is so important for us to have the other security project on the side that actually look into that and see how it kind of match up to the rest of the parts of the network.	TS

55	AS	So, do you have any future plans for the security issues or?	
56	R2	Well as of now we don't know what the issues are so. But obviously if there are any we have to adopt. So, I mean the plan we have at the moment as we are still running as a test-bed or kind of a in a small scale before rolling out. We hopefully have coming out from the other project is that we have a architecture of how the security solution has to be implemented over the whole system. So, I mean, hopefully we will get, maybe not a whole solution but large part of the solution from that project that we can implement on the test-bed afterwards to make sure that we have fully complete system. From the end-sensors all the way up through the systems into the cloud network.	FS
57	AS	Do you want to add something that we have not talked about?	
58	R2	No, but I would like to... Since you are really into the security and the kind of mid-degree of that I think it would be really beneficial for you to talk to the guys running the security project.	
59	AS	Yes.	
60	R2	They could probably give you some more that would help. To answer more questions.	
61	AS	Yes, absolutely. I was thinking about training and education; do you work anything with that in the city?	
62	R2	Yes, we do but we haven't done it when it comes to security in that sense. But we have been working with, we have had training for instance how to use the different kind of networks, and how to connect sensors, how to build it up. And that is something we do both towards… I mean we have had open classes when it comes to use the lower network. But we also at the moment work together with one of the, is it high school, gymnasiet?	RPLS
63	AS	Yes.	
64	R2	Teachers there, to make sure that they can actually use the open platform and test-bed that so we build up in the city to use it in the correct column in the school.	
65	AS	Mm. Yes, I think it was really interesting the things you talked about to build a trust and tell citizens about what the issues could be to use it.	
66	R2	Yes, I mean even if we kind of think that we have full control it will always be stuff that can go wrong, so I think	RPLS

		if you are only open at beginning and what you do and what you are trying to do and they still want to be part of it. I think there are much better understanding of when things go wrong.	
67	AS	Yes.	
68	R2	Otherwise, if you kind of try and say that everything is safe, and nothing is never going to be wrong and something goes wrong. Then you have large trouble trying to get those peoples trust back again. So, I think that is much better, I mean it is like when you have the bike trial. I think we got some 600 people signing up just in 2 weeks. Because they saw that the benefit, they got out of it was bigger than the threat of actually someone looking at how you are using your bike every day. So, I think, there is also something you have to show. What do they get out of it? If you can show that it actually have something more to it, they can gain more than they are actually going to lose. It puts you in a better position.	RPLS
69	AS	And in this case, you could tell the people that participated but how is it possible to do it like in a bigger area, like to all the citizens?	
70	R2	I mean if you want to try and if you basically want to use all at the same time?	
71	AS	Mm.	
72	R2	Yes, I think. Basically, I think if you do this small-scale test first hopefully you will find things that goes wrong in that sense and then you can feel more secure once you rolling it out for all. And then, again, when you roll it out over the whole city you have to be open again and tell people what you are doing and why you do it. Things can always go wrong but as long as you are open, I think it is much easier for you to handle the effects of what went wrong. And then if you are trying to just not telling what you did.	RPLS
73	AS	Do Lund have any specific goals about the smart city? Like the city in itself.	
74	R2	I am not the expert of these goals. At least there is a lot of sustainability goals in Lund. I don't know if there is any, I mean smart city in such a broad perspective. But a lot of the goals are about when it comes to sustainability. And Lund is really pushing towards being a sustainable city in all kind of stuffs so there we have some hard goals. But in other perspectives I don't know if there are such goals to achieve.	

75	AS	Okay, thank you for your time.	

Appendix 4: Interview 3

Job position: Senior Project Manager, Mobile Heights
Located in: Lund
Date: 2019-04-24
Duration: 48 min
Language: English
Type of interview: Face-to-face

R3: Respondent 3
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	You started to talk a little bit what you work with and do you want to explain a little bit more about it?
2	R3	Yeah I mean, in the smart public spaces we usually talk about collaboration between the public organizations and the private companies and how we tie them together with projects that the public sector can take use of. So that is the basic idea of this project. The aim is also one other thing is that the people that live in the city should take benefit of it as well. But first they need to have some kind of basic setup and then it will grow and in the end, it will enter the people in the city as well. We build about technologies and try out different technologies but technology what is important is that we, what you say, we do things with the technology it is the thing we do, not the technology, I mean the use cases are more important than the technology. Then we of course would like to try out new technologies as well when we do it because that is two sides of things that happen in the society. One is that you have to develop the society in the way of how to live in the city and the other thing is that we need to develop technologies that can help out the society, so we try to do both.
3	AS	How does it work is it Lunds kommun that order something that they want this or who decide?
4	R3	It is, probably R2 has answered this and I hope I can answer this in the same way but the idea is that anyone can come up with ideas so it is free for anyone to come up with an idea of what we would like to do and then we try to tie this to the public sector and sometimes it don’t and sometimes it does and then we sit together and see how big is this use of this project and what is the gain for all the different parties that are in this project and what of technology level it is and then we take a decision, we go for this project. And we also would like to have four projects at the time running through this chain and the aim is 6 months per project but it has been turned out that the projects have been bigger than six months and then we take certain to evaluate it and then the project is basically longer. Some started one half year ago and is still running, due to that the use of it in the public sector is still using the project because they got use of it.

5	AS	Okay, and R2 described that you are responsible for the security in the projects.
6	R3	Yes, so the public spaces this project will utilize anyone that can elaborate new technologies. Mobile heights together with RISE and Sensative and also u-blox started up a discussion how do we secure the sensor that to make sure that the data come from the sensors to the cloud that it is completely secure. We need to trust the value. No one can hack the value and also make sure that the value is correct when it arrives. And that is why we started this to have some object security system so the object is secure so even if it is jumping between different technologies it is never revealed information so the information will be untacked and you will not be able to reach it without the encryption keys and that is the idea to make sure that even the jumping between different technologies it will be secure. That is not the case today, there are many different security protocols that you can use today that can secure A to B one technology. For example, Bluetooth has their own but when you change from the gateway to internet protocol the gateway will open the data and then attack the new security way and that is something, we would like to tie to have higher security.
7	AS	Yes, that is something we have found that with the Smart Cities that there are so many different technologies so there is a problem to like to make it sure between all of it.
8	R3	Exactly, the end date of this is in December so we have the really good security people working on this and that it is good proposal that hopefully will be the standard, so there is a proposal for standard but maybe know how long time it will take before it becomes standard and that is a process that has been used for certain time to make sure that no one can hack it and is stable and so on. And then it became standard so you make a proposal and everyone use it and try to hack it and so on and not suddenly it go through all the steps so hopefully we have in small scale extremely small scale one sensor and one node that have been proven that this protocol will be used but build it in a real environment that this project aim and goal in this case to go through all different kind of technologies and that has to be done before so that is a big trial that we try to do and then we use standard components from the industry not special things. This is real stuff that you can buy from the market. So, the idea is hopefully we try to have something that anyone can use in the end of this year.
9	AS	Sounds good, do you want to describe this a little bit more how you do this? You have a team?
10	R3	Yes, RISE that are the experts in this protocols or security, we have u-box that have started looking into it because they aim for a very good high-quality modul. Moduls for automative and everything like that and then they would like to have high security level as well. So they started to look at for example before so they have started it but they have not entered the product level yet and make them work together with RISE because RISE has been testing this in labs, they have the building blocks which we will build into u-blox modules. At the same

		time I mean u-blox has with their technology, the hardware and so on they have one part of the line of the information flow then you have the other side when you come closer to the cloud, we have Sensative so they are also working together with both u-blox and also RISE to understand what is the kind of information and how to support this. This is not simple. But it is simpler to add it because they will not, they will just see it as a data flow, but they need to fulfill some kind of API standards so they actually can handle the data and then encryption keys. We have not added any distribution of system of encryption keys yet, that is another big project that actually Sensative, HI?, RISE a bigger project they work on how to distribute keys when you have many different users in the network but that is not our case. Our case is to test from the sensor to the cloud to make sure that it is encrypted. Then the key, you can add that into this later on, when that project has finished.
11	AS	It feels like you have experts in many different areas?
12	R3	Yes, the teams we are working with, the companies in this area, the competence is extremely high, and I would like to say, people say that we are one of the worlds, in the front when it comes to IoT battery-driven sensors or devices.
13	AS	How long time have you worked with Smart city initiatives?
14	R3	Since I started at mobile heights two and a half years ago. And smart public spaces actually started with a pre-study one year and I was not their writing this application but when we got this I just started at mobile heights and that was exciting because no one knew what was going to happen and there were no systems set up and thinking at all, so it has been growing gradually in the mindset of the people in this project so it is really nice to see how it has developed just the mindset of how to work with this. My background is from Ericsson modem part, so I have been in the top floor in that building, many years ago.
15	AS	Okay, you have not moved so far.
16	R3	That is always a tricky question. There are two areas, I see that people mixing up the technology and the people, they would like to put everything in the same basket. I don’t think so, one thing is that you have the smart technology that is there for the people's sake but the technology has to be easy handled, you should be able to, maintenance should be easy, it should be easy to exchange sensors, and some part of the system so the management of this technology has to be made in a way that is flexible. When it comes to the people you should not add technology that the people don’t need. That is also something important. The people should be able, it should help the people to be in the city. A Smart City should be something that you as a person to simply be in that city, you don’t know really why, it is simpler, you have that information at a certain place and time when you need it, and also when it comes to how you move around, make sure it is safe and clean and everything. I mean to lower the amount of people that is moving around, or the vehicles, bicycles whatever it could be in the city you need to think about

		the logistics in the city and everything like that. How do you empty a dustbin for example, do you need to empty it every second, day, week? Yes, some places you need to more often but some maybe it is once a month and then you optimize with the technology to make it better for the people. That is what I see as a Smart city and that is for the environment, this technology will help the environment. One more thing I would like to say, ah tit will come.
17	AS	If we should dig more into the security, what are the security issues and challenges according to you in the Smart City?
18	R3	One thing is of course to make sure that you can trust the data. But one thing that crossed my mind, one and a half year ago in the beginning of the smart and public environments 2 is that when you have a lot of information in the city you could actually be able to track people with cross coupled information and that is something that is very hard to prevent. And something that crossed my mind that time as well is that the only way to do this, not the only way but one way is that you can add AI to be able to see if you try to track people, you extract data from different cases from one place and then you have us mind that you would like to extract this data to be able to track that people. And that is something that you have to, in some way have a system that learn that when you add new sensitive data and so on, you have the system, has to learn how you track people. You get so many nodes that you can't handle that in manual way, and if you block this technology you will stop the evolution of the development of the smart city. And then the people will then not get the use of the technology that they could get use of. So that is a lot of that kind of stuff that is the problem in some places. You need to make sure that you do this in the right way otherwise it could actually, bad people can use it and that is something you, that you have to think about. The data can do harm as well and that is something that the city has to think about how to ensure that. So in the beginning before you have this technology when you set up sensors and so on you have to think about when you open up the data make sure that together with other data, you do not open it if you can track people until you have a system that can handle it. For the city itself they get access to the data and hopefully they will not track, we are not in China.
19	AS	Yes, I also think that R2 mentioned it. Yes, a lot about trust.
20	R3	Yes, one of the project is to tracking bikes and how do you show this information they have each individual person has written it is okay for that company get this information because I have nothing to hide but that is for that company because they are trusty. If that data comes out and you can find this on the net you could start track and find where people are working, where they shop their groceries, where they live, which kindergarten they leave their kids at. Then the people can track exactly the pattern for each individual person and then suddenly you get different angles how you use that data for commercial purpose, and so on and then they will nag that person in the end with advertisement and that is not nice. So, we are filtering the data so you will not see the end and start, the start and stop, we cut the information that will be

		shown on the visual page to make sure that we will not reveal the sensitive data.
21	AS	And that is just one project with the bikes?
22	R3	Yes, that is just one project I mean when you combine this with other, you have to be careful.
23	AS	Yeah. You have not really implemented something in Lund, you have the bikes is there something more?
24	R3	Yeah, we have the bikes, we have the sensors to measure the soil moisture and temperature in the air. We have the big belly level measurement for sensor the renhållningsverket that will collect the garbage in those big, we have these the fourth is the surveillance of the critical infrastructures, we are testing extremely new technologies, the Bluetooth mesh that is not yet out in the market in a good way so there has been NB-IoT it is also new there is only Telia that has launched NB-IoT in Sweden and it is also getting updates that it is, now it is working and now it is not, due to updates in the network but that challenge the technology as well. The other project is not extremely technology driven, lower based systems, we have an easy Bluetooth button for the phone to track when something happens on the roads for the bicycles or the people that walk. That is not very high technology level on these, but when we try new technology like Bluetooth mesh longway, the first chip available at the market available was on September/October something and then you have to build the hardware and so on then you figure out we have updates again, just a couple of weeks ago we need to figure out new hardware, that is a little bit tricky to deliver within six months so we are a little bit behind in the schedule but we are soon there. So, the idea is to set out sensors out in the metacase boxes you have electrician from building to building, the grey boxes are a little everywhere and put sensors and network nodes in those will make a mesh network nodes with those cabins in the areas of the city. Where you have a lot of different kind of sensors so you can mix different kinds of sensors to connect the same network, that is the idea.
25	AS	Yes, because we had a question if you had had any cyberattacks against these systems?
26	R3	No not yet we have not seen any.
27	AS	Do you have a plan if something would happen?
28	R3	There is currently, I would like to say it is quite funny if they would try because then you learn. I would say it is extremely uncritical data. You can learn how they do and what we need to do so but try to hack it. It is not so complicated to hack it today because we have not added the full system. The experts can do it, maybe not ordinary engineers they can’t do it, we are using the standard security protocols that are available today not the most advanced ones. And the most advanced one you basically need to open up, log the information in certain places to be able to hack it.

29	AS	So, it is just the best ones that are able to hack it?
30	R3	Yes, but there are, they made an analyse of this network that critical infrastructure, and how many vulnerable we have in that one before we started and that was a few and that should be fixed and sorted out.
31	AS	But how would you think if you had an attack with the security, how would it affect the privacy and the citizens?
32	R3	Yeah if you hack one sensor it will not happen that much, if you don't use that sensor to send out a lot of emails or something like that to use it as a way in, where you can get in and get access to all the other data. With this system we have today with those few sensors it will not affect it. Because the filtering of the data that we show on the screen is filtered in not in this, it is filtered before, so it is not in the tool we filtered it. If they hack the files with the data, they will not see more than is shown on the screen and is already open so in that way it should not be jeopardizing the privacy. It is more that if you use this information to control things and then you change the information and then you control it in different way, that is a different story. Right now, we are not controlling things so should not be any problem today.
33	AS	Okay yeah, I have one question about the technologies in the smart city, what do you think pose most security issues, like the IoT, the cloud or?
34	R3	Eh, if you think about doing the security of things if you add security in IoT device that should be safe and then I mean I am not a security expert, that is a tricky question. Because in normal cases today the most vulnerable place is the IoT device because people are not adding the security so adding the security that is available on market for example take the home network, the Wi-Fi, how do you make that secure? There is not so many that have secured their wi-fi. I am not allowing anyone access my wi-fi by a new device because they don't have the right address, but how many do that for example, not that many. But that is not fully secure anyway because there is a way to go around that one as well. You need to add security at all levels. The system is not better than the weakest link so if you add the security everywhere were it is available, I don't know. I mean there are security systems today that can handle a lot of things on the cloud, it is more mature on the cloud than on the device.
35	AS	What are the hardest issues for you to tackle with the security?
36	R3	I mean the security of a system is never ended, you have to continuously working with the security because new things are showing up, people are finding new ways of hack it and so on and you need to keep them updated. That means that when you create a system you have to be able to in some way update the units and that is something that is for example critical infrastructure. All the way down to the sensors to have the security updates available all the way. If you can't do this updates sooner or later you will be hacked that is simple. That is the key, be

		able to maintenance the security on the devices, the system and so on regularly and monitoring the data. The monitoring the data also the AI thing i believe, the AI can actually listening to the data, that the data is suddenly very strange, it is not only standard pattern, there is a cloudy day outside, why is the temperature going up in that cabin suddenly? Yeah it could be that it is a fire in it but little small increase and that is very strange then even if the sensor is spoken something has been replaced by another sensor that is sitting in different place, that is normality, you need to kind of detect in the future.
37	AS	Okay, we have already talked about the solutions for the security, you talked about the technical solutions with encryption and filtering, do you use anything else there?
38	R3	Yeah another thing is that there have been in discussion, it has not been very much discussion, but what sensors are we going to use what kind of actors are we going to use, you have to certify those in different levels depending on what security level you would like to have on these. So, if you have a simple sensor that is, for example measuring temperature, it is not very sensitive data and it does not need to be very reliable and no one is interested in this kind of data either. Those could be easy certified, you just need to add it and it will work in the network and then you can increase those two or three steps with the advanced object security setup. And then on that you could add the data analyse logger.
39	AS	So, you have taken that into consideration what data you use?
40	R3	Yes, the certification of the sensors is very important as well, to trust the data, the sensors itself. It doesn't have to any people that would like to do any harm, just the sensors.
41	AS	Yes, I do not know if you work with this or if it is more Future by Lund, but privacy by design and security by design is that something you do?
42	R3	The companies working with that the companies within these projects need to work in that way because that is basically the law more or less. For example, Sensative they have built in to not handle any personal data at all and they are not looking at the data just the switch for example. That is a way they have solved it. U-blox for example they just take the sensitive data and send it out to the Sensative platform and then the users get the data. They don't look at the data, they don't care at all because they don't own any of those kind of data, just the use of the data. If you take Trivector that is with the bicycle data, they work a bit more when it comes to this and have agreement with users that will give the data but we are not from a project point of view looking into design, for privacy in the same way. It is always in the mind, this discussion is coming up in all kind of discussion anyway how do you make sure that the privacy is kept. The mindset, the discussion is there every time we handle data.
43	AS	You said you talked a lot about it, do you have any education or training about security and privacy?

44	R3	No that is why I am not going into technical details; I will leave that to RISE and Sensative and u-blox that is a lot of those technological discussions that are outside. If you see the overall picture, I have worked with this sometimes, but I have no special training about the security.
45	AS	Yes okay. When you, it feels like Future by Lund is more the connection between different stakeholders do they, do you know if they set any goals for you with the security and that you should test?
46	R3	Future by Lund is not involved at all more than that they have the smart and public environment project that will be used in that so there is a collaboration in that way. But that is something that I and RISE suggested actually, it's one and a half year ago. We need to do something about security, some project regarding that because that happens a lot and it’s, there is still past to go when it comes to IoT devices, and we said okay we need to find something and then Vinnova had an application to search for. And that is why, let’s do this and then we gathered with a couple of mobile heights members.
47	AS	What solutions would you say are the most important ones that you have for the security?
48	R3	About technology or the data. You have the security of the technology, make sure the data is coming through and then you have the security of the data, how do you handle that data in the cloud and so on. It is equally important because if you get in anywhere you open up the full system so I can not say that one thing is more important than another because if you find a hole to go into it doesn’t matter where it is.
49	AS	And what would you say take the most time to do with security?
50	R3	Test it, it is never a test end. Systemisations is very tricky and the key distributions those things are the researchers working a lot with so that is something besides testing is quite much work.
51	AS	Do you have any further plans or future plans of the security how you will tackle this in the smart city?
52	R3	When we have a system that works, we have a lot of sensors outside I would like to put the AI on it because that is a simple, no not simple, something that is closest as a next step. Always develop the protocols to be more and more secure. But I think the solutions we try out now is what we are going to live in many years in front of us and then you need to have another security to make sure that the sensor is reliable that is one and if you hack any in some way due to very tricky circumstances you should be able to detect that. Be able to analyse the data flow and that is all, is big data flow and you handle that. If you talk about ESS they have 1800 sensors always continuously control of them, you can’t have people for that so that is what is going to happen with the sensors in the city, you can not have people that sit and analyse the data and if you not analyse the data and make sure that the data is correct then the system will be unreliable and who would like to use

		an unreliable system, no one. And then those sensor networks will die. So you need to make sure the security is there to make sure the data is coming up is reliable then if someone try from outside change the data or the sensor itself its bad, it doesn't matter you have to have a reliable system, that is something that take a lot of effort.
53	AS	Great, I do not have any more questions. Do you want to add anything?
54	R3	It is very exciting with the security because there are many things to do and a lot of things that is going to happen.
55	AS	It is a hard subject.
56	R3	Yes, it is a hard subject.
57	AS	But to summarize it, it feels like Lund they have really thought about it and the things you do is prevention before something happen and you have different technology solutions and you also evaluate the ones before you implement the technology.
58	R3	Yes, so when you choose the technology, make sure you choose the technology that support the security.
59	AS	Thank you so much!

Appendix 5: Interview 4

Job position: Smart Region Program manager
Located in: Copenhagen
Date: 2019-04-24
Language: English
Duration: 43 min
Type of interview: Telephone voice call

R4: Respondent 4
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	Hello, it is Sofia again.
2	R4	Yes. Hi.
3	AS	I am happy that we could make this interview by phone instead because we had some issues earlier so we couldn't make it in time to Denmark.
4	R4	Yes, that is fine.
5	AS	Yes. I can start talking about us. It is me Sofia and my thesis partner Amilia and we are studying here at Lund University. We both have a bachelor’s in information systems and now we are studying our master. So, we are doing our thesis now and our thesis is about Smart Cities and Security issues in the cities and what cities are doing to prevent these issues that occurs.
6	R4	Mm.
7	AS	And like Copenhagen is one of the cities we want to research in. It would be nice if you could talk a little bit about yourself.
8	R4	Yes, well I have been with the capital region for almost 4 years. I don't know if you are familiar with the political organization in Denmark on a regional level. It is somehow similar to, to Sweden.
9	AS	Okay.
10	R4	You have the city-level and you have the governmental level and then in-between you have the regions which kind of handle things in between but mostly getting the cities to co-operate in different kind off issues. And I have been building up this new area which we used to call smart growth, which is basically about smart city. I started in the region 2015, and a new regional strategy was being made and we had a specific chapter on smart growth. I have been working for many years at the government, national governmental level. Last I was working in the Danish Business Authority where I started the government work on Big Data and I was working with Internet of Things before I left the Authority. I have been with the national IT and Telecommunication Agency for many years. I did some work with OECD and the European commission on digital infrastructure and digital economy. But as a representative from the Danish government. But now it is the region and I work more closely to the actual projects in the field and are not just writing notes and governmental strategies. But as I said, when I started, I started working on a strategy for the region where we had a chapter on smart growth were we basically had a focus on five pillars which is something I more or less have been working on since my time with the

		government. The five pillars are basically a focus on digital infrastructure and how to make connectivity for both humans but also robots and things available everywhere in the region. The second pillar are data, both data infrastructure and the collection of data, sharing data and how to handle data and other things.
11	AS	Mm.
12	R4	And as a third pillar we have a focus on IT security and privacy. Fourth, we have a focus on digital skills and then there is, a focus on strategy - which was a part of our original strategy and the chapter on Smart Growth witch I mentioned. Moreover, we launched a Charter for a Smart Greater Copenhagen in November 2018. The strategic level is about making actors in the cities, companies, research institutions work together on a common framework in the regional development when it comes to digitalisation or use of data and technology.
13	AS	Mm.
14	R4	Ehm. We basically started out with doing analytical work to find out our focus on digital infrastructure where we were starting with challenges on the basic mobile and broadband infrastructure but also how to take it in an overall infrastructure with also low frequency networks and so on. We started to work on a data hub and how could we have some common work on what to do with data, both when it comes to getting more public data available for free both also start using data.
15	AS	Mm.
16	R4	on top of these analysis we started with some projects. Both on data, digital infrastructure, IT security and privacy, digital skills and the a strategy project. And we ended up being four people in a team starting op several digitalisation projects about using data and technology. And that is what I have been doing for the last 3,5 years. But the last six months we have had a re-organization because of changes in the national regulation. This means that the region cannot do work which is related to creating growth and jobs.
17	AS	Mm.
18	R4	We can do work on regional development but not when it comes to pushing businesses to scale on hiring more people and so on. And we cannot take an overall lead on the digital agenda or digital transformation projects. We can only do work on digital and smart work as long as it is supporting our sector areas which by law is our areas of responsibility, which is the mobility area, where we work to have a more coherent mobility system in the region. And the area of environment and climate, education and health. So, when we do smart or digitalization work it relates to these areas. Now we are in a new strategic period where we are going to decide on what is our digitalisation aims for the coming years. But we are waiting for a national election to take place because the sitting government have put forward a proposition to close down the regional political level as a political entity and replace it with steering groups. But only regarding the health area whereas environment, mobility and education will be transferred to the city level and/or national level.
19	AS	Mm okay, when you talk about these areas do you have any initiatives implemented now in these areas or are you planning to implement in?

20	R4	It all depends on what will happen with the regions after an election so if it turns out to be a change in government from a right-wing government to a left-wing government there is a whole new situation because it is not the plan of the left wing to close down the regions. So, so we are more or less in a period where we wait for this national election.
21	AS	Okay.
22	R4	But it doesn't seem to go so well for the right-wing government. Taken an election today they would probably lose. And then it could mean something new for the region, but to focus on the sitting law there has been made changes where we cannot do digitalization work for, just for the digitalization itself. It has to be about improving mobility, environmental challenges, climate, education.
23	AS	Yes.
24	R4	And…so in our new strategy, the digital transformation or smart city work would be a part of, kind of a innovation toolbox.
25	AS	Mm.
26	R4	Where we can initiate some initiatives. But we don't have the same finances as we use to in our strategy where we would focus on creating growth and jobs. Many funds have now been transferred to the city and national level. So that means that when we do projects, we probably will only do initiatives on each sector and then we would do some cross-cutting work where we develop, for instance digital tools and platforms and the digital infrastructure necessary to solve the mobility challenge, the climate challenge and so on. And we also try to tab into problems with this cross-cutting focus such as if we could begin to combine specific key indicators in digital mobility initiatives which has an influence on for example the Co2 level. Which then again could have an influence on citizens health, for instance living on a heavily trafficlly roads where the congestion would then be changing and then the health conditions could be changed. So, if we could include several solutions and kind of solving several challenges on different kind of areas and harvest synergies of a better overall picture by using data from different kinds of solutions and from different sector areas. So, we could not only have less congestion but also better health, climate and so on.
27	AS	Okay. I wonder here. A smart city, it is defined in different ways and what is a smart city according to you?
28	R4	Well. Yes of course there is challenges on defining smart, that is often very broad concept. Probably all sectors will be included in smart eventually, then it will have no meaning, so in some ways it is better to talk about digitalisation. So, when you say smart city is in a way about digitalisation or digital transformation. But when it comes to region, we are relating the smart to the sector areas are our areas of responsibility. So, smart city is about creating a better coherence in the public transport, it is about having education and meets, the regional needs. It is about sustainability, it is about re-use of the sources, it is about digital health in the health sector. So, the patience will experience a better connection when they move from one local health institution to another or from the city level to the regional level – for example from the local doctor to the hospital. And then of course smart city would have some cross-cutting focus areas related to data and technology. But the, if I would say it in a short definition a smart city (or region) would a be a region that promotes a green and innovative metropolicy by using data

		and technology in partnerships in a secure and ethical way that solves some of our challenges in our society and increases the quality of life.
29	AS	Okay.
30	R4	And of course, that would include many things, but we in the region can only do it within these four sector areas. Mobility, environment, education and health.
31	AS	So like, in the smart city initiatives in Copenhagen, what are the security challenges? Like information security and cyber security challenges.
32	R4	Eh, yes well. Challenges is closely connected to more and more things being connected to the internet. So as more and more things are connected, kind of the vulnerabilities increase and so what we do on one side is to build in IT security from the beginning in our solutions. On the other side it is about connecting and handling all the data in a ethical way the protects privacy - which means that we have to handle data in the right way even though no one is looking. So, we did, one project we work on, where we have been trying to more or less build in privacy and security from the beginning. And we have established a Smartcity Cybersecurity Lab, SCL. We have a secretariat running the lab at, our technical university [Danish Technical University, DTU]. And we have just recently launched a hackerLab were we do projects, where we try to link other digital projects in the region to this Smartcity Cybersecurity Lab and they will do some test of different elements in the projects. And students moreover have the opportunity to try to hack different kind of things. Just recently, we had a hackathon where for instance another project we have set up that uses the same LoRa technology network could be tested by hackers.
33	AS	Mm.
34	R4	So, at the hackathon they could try to hack the LoRaWAN network, they could try to hack a self-driving bus which is also a project running at the technical university where they have the bus driving around the campus. So more or less it is a track which we link to other projects to make sure that, not just in theory but actually in practice we think about IT security and privacy.
35	AS	Okay.
36	R4	But in many solutions, the companies are responsible for the IT security and build in from the beginning but we for example at the hackathon are trying to also make a better link to companies who could then solve some of the challenges we have in the public sector and which we put forward for private companies to solve.
37	AS	Mm.
38	R4	Companies can kind of try to make solutions for these challenges we have. The technical university just recently had some funding, I think more than 20 million DKK to make a cyber-hub which could do all these things when co-operate together with private sector. But as I mentioned earlier the region cannot do work directly together with companies when it comes to this area about growth and job. So, we will not be working in this part, but could be done by universities and/or some other partners, that link up to the smart city cybersecurity lab.
39	AS	Okay.
40	R4	In the overall organisation.

41	AS	I was thinking have you had any cyberattacks that you know of to the smart city systems?
42	R4	Ehm I think it is too early to talk about cyberattacks in relation to our projects because it is pilots.
43	AS	Mm.
44	R4	We have not moved into operation. So, so... we are in more secure environments.
45	AS	Mm.
46	R4	So, the cases I know of is more like cases that comes from the national level which has many cases of hacking of different kind of solutions. It could be linked to the smart city area and they have had some reports on things being hacked and they have some cases you can read on their own web page which is possible to download.
47	AS	Mm.
48	R4	If you want to look into it. The reports are in English or Danish I do not know.
49	AS	Eh like when you implement these projects have you thought about how you will handle attacks if you get any cyberattacks?
50	R4	Ehm I think some of these projects there are also some guidance on the national level. Of course, from the GDPR legislation there are some things we need to implement in every institution, no matter if you are private company or public sector, you have to have some procedures for how to handle attacks. And of course we have that in our own organization and our other partners have as well…but again, when it comes to our actual projects it is pilot, so of course we are in a closed or safe environment with a different setting as long as it is not in operation but of course we think about it and how we should handle different kind of challenges. But it would be the cities, city of Copenhagen, city of Frederiksberg and so on, that would have some actual digital solution which have implemented or have dialogs about attacks etc. Copenhagen also have a advisory board where they have the board discuss different kind of problems related to privacy before they roll-out a digital solution.
51	AS	Okay. I was also wondering, you were talking about, before that Smart Cities use smart technologies like IoT, Big Data and also other stuff. What technology do you think are posing the biggest issue for the security in a Smart City?
52	R4	Well, of course health is a challenge because it could be a matter of life and death. People getting wrong medicine and so on, or wrong treatment or whatever. The same counts for transport if you could more or less set up different solutions for the mobility in the region that make the mobility very effective and optimised it would have severe consequences if it would be se out by an attach. Not only economic challenge but also it could take over self-driving car or whatever where people could die etc.
53	AS	Mm.
54	R4	And the energy system. If you could shut-out the electricity of things. So, I think that you have some major critical areas which you could basically close down and maybe more or less a whole society.
55	AS	Mm.
56	R4	Which yes have several consequences, yes.
57	AS	Okay, and do you think the security can affect the privacy of the citizens in a smart city? And in a what way?

58	R4	Yes, that is the critical part. It is not only important to make sure you collect and handle the data in the right way. You also have to do it in a way that supports in Denmark our basic values which means democracy. So we have to do it in the right way also so a citizen can delete their own data or make sure that no one has information about them that they don't want to... or analyse in a secure way. Of course, it is a trade-off on how long you can go on the innovation side and at the same time have a high level of security. So, it is a trade-off, but it should be possible for citizens to... yes as you make choices in all different kind of ways of what information you give about yourself. You should also be able to do that in the digital world.
59	AS	Mm. I was thinking, how do you think privacy breaches can affect the smart city systems?
60	R4	Eh, it could basically make it difficult to do new projects and have funding for projects. If suddenly there is a fear of big brother society where no one can be sure around another.
61	AS	Mm.
62	R4	And trust is gone. It takes long time to build up trusts between people and only short time to destroy it all. And if you have done that it will take large amount of resources, initiatives and so on to build it up again. So, I think it is important to do it in the right way from the start and that boarders necessarily between that new things should be an open book and, and, but that you have enough information for citizens to compute and take decisions on the information they have.
63	AS	Mm.
64	R4	Because all information is not necessarily the right way.
65	AS	Mm.
66	R4	There could be more confusing, for instance if you are completely open on different kind of algorithms that could actually lead to less trusts. So, I think it is a balance and it is something which should be discussed on different kind of levels including or involving the citizens and so on to make sure that you have been around different kind of arguments before you...
67	AS	Yes.
68	R4	Go for a national solution.
69	AS	Mm. Yes, we have been a bit into the solutions for the security and privacy issues but could you explain a bit more how you…Because you are like in the beginning phase, like the pilot face of your projects. How do you plan to work with security solutions in the Smart City initiatives? Or do you work with it already?
70	R4	Yes, as I said we try to work closely together with SmartCity CyberSecurity Lab when we start our new project more or less coordinating the different kind of activities with our smart city cybersecurity lab. So, for instance we started off a new project in secure and we used data where we have a track on LoRaWan-network where some cities have put up a network in some areas of the city and are trying out some different kind of sensors solutions.
71	AS	Mm.
72	R4	And then at the smart city cybersecurity lab they work on a hacker lab for security and privacy issues in which they do… yes, see if they can the hack the system and come up with data solutions and so on.
73	AS	Mm.

74	R4	But of course, when it comes to buying from the shelf, these products from private companies they usually have thought about different kind of IT security and often comes up to making sure that it is always update, basic software, steering operating systems installed and so on.
75	AS	Mm.
76	R4	Of course, no solutions are 100% sure. So, it is also about, thinking about what could happen between... linked... suddenly we are hacked and so on.
77	AS	Do you work anything with privacy by design and security by design in your projects?
78	R4	That is kind of the idea of linking projects to the smart city cybersecurity lab that we use to work on different projects as privacy and IT security as privacy by design.
79	AS	Mm. Okay, do you have any education and training for the staff and also for the users of the Smart City systems? It could be like both staff and developers, and also citizens.
80	R4	Ehm. Yes, not specifically focus on privacy and security. Of course you can study at the university... I mean dataration and some of the people involved a bit in the smart city cybersecurity lab is runned by a professor. And some staff and students. And there is, as I also talked about being this link to private companies and so in this work, yes, there is something about the IT security and privacy, but you have this project called "ready for smart growth".
81	AS	Mm.
82	R4	Which was trying to make personnel from the cities more competent or skillful in handling different kind of smart city solutions on a practical level. What is it and how can I work with it, how can they make a strategy for the city. And also, there were some practical part to it where they actually could see some solutions put up in our lab – DOLL Living Lab, which is the Europe's largest smart city lab for urban smart city solutions. The lab have more than 100 smart solutions installed.
83	AS	Mm.
84	RS	And it is increasing all the time. And a lot of project we have, there is a focus on how to, to share competences, skills between cities. We haven't found out a model of how to do it yet.
85	AS	Mm.
86	R4	But the idea that it is difficult to achieve it. To think about this, to do it together and share not only data but also the sources and competencies.
87	AS	Yes, and this is like competences around security then?
89	R4	That also would mean security, but I think... mostly cities would have someone knowing things about GDPR but when it comes to more advanced IT security and privacy skills, I think we would need to co-operate with researchers or private companies, experts in this field. But also, how we more or less try to work together with, with the public sector, the private sector and researchers to resolve... cities have different kind of interests.
90	AS	Mm. Do you have any specific goals related to security in your projects? And do you, and do you also test, security test the systems?
91	R4	Ehm, yes of course there is kind of a set that's when we do the pilot test, but it is also close related to company's development kind of solutions. We have a project on a common datahub, The Regional Datahub.
92	AS	Mm.

93	R4	Where we have different kind of tracks among others. One on mobility, and on this track private companies are developing some prototypes which should be able to solve concrete challenges in specific areas in specific cities where they set out an environment to test solutions. And it usually will be a company who builds the solutions in a secure way, and responsible for the product but of course we do need to think of privacy and how data are handled when data is used by the city, we thinks of how this should be done in the best way. And then we consult and test from our smart city cybersecurity lab.
94	AS	Mm. What solutions for security do you think are the most important ones?
95	R4	Ohhh, that is a big question, uhhhm. I think it depends much on the actual case you look into. Because when we do projects, we always morely start with a challenge. So, before we do the platform or a tool, we think about what we could solve.
96	AS	Mm.
97	R4	Which interests have a part in this and then we try to build a partnership around this and then first see, we think about module aspects. So that would also mean the solution, in what way would the data matter in private relationship, then we talk about we need parts of their certain needs in some part of a critical infrastructure so there should be security therefore and so on. So, I think it is a… we should think about it in the beginning but as long as it is a smaller pilot project, I think it is not so essential in a solution about security. We see it is kind of the, the solutions we are about fine and then we see what kind of the gains and the value of the solutions are, possibly differently. And then we put scale and make it for the ones who operates it, but we are not there at this level. We don't have scale solutions in all of these. But of course, we are beginning to see somethings, especially in the mobility area where we use traffic-lights and so on.
98	AS	Yes.
99	R4	So, what are the most important? Well, in relation to privacy it would ethically be about the way over our head. In relation to security, it depends on what are the critical infrastructure then of course it is important but there is... if it is a matter of life and death there should be not only one solution, there should be to have a voice in security.
100	AS	Mm.
101	R4	But, yes. I think it is too early to… Eventually if we one day will have this part in the digital world or... yes, to move around in a more doing all kinds of things. Of course, it will probably be quite essential for our society, just as having electricity and physical infrastructure for transport and so on. What would be quite essential... One day when we are probably when we are quite efficient, working in a digital world it will cost a lot of money and mean big... yes and also bad things which would close down.
102	AS	Yes.
103	R4	It will be more essential than electricity but of course it would be built on, on electricity too so.
104	AS	Yes. I think we are quite done with our questions now but do you want add something more that we have not talked about?
105	R4	No, I am not sure, do you have some question that would be interesting to now a bit more about?
106	AS	No, I think we are quite, we are quite satisfied with our answers so.

107	R4	Yes.
108	AS	I just want to ask you also; do you want to be anonymous in our study?
109	R4	No, that is not necessary. You could... it is fine to mention who you have spoken to.
110	AS	Great.

Appendix 6: Interview 5

Job position: Sustainable Business Hub
Located in: Malmö
Date: 2019-04-25
Language: English
Duration: 32 min
Type of interview: Face-to-face

R5: Respondent 5
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	Is it okay if we record the interview?
2	R5	Yes, it is okay.
3	AS	Do you want to be anonymous in the study?
4	R5	No, it is fine.
5	AS	If we start with what do you work and what do sustainable business hub do?
6	R5	Sustainable business hub is a cluster which means that we have a network of members, we have 85-90 members, most of them are private companies, SME small and medium enterprises but also large companies Eon like and Skanska we also have public organizations, authorities and also municipalities like Helsingborg, Malmö and Lund and we have a few from academia and research institutes like RISE and about ten person working at sustainable business hub and a lot of our daily work is in connection with projects so we have a number of projects, 10-15 different projects in our area of interest. And our members areas of interest. These projects are normally financed through EU or Swedish state funding, Vinnova is our main Swedish contributor financing. And our main fields of interest are sustainable cities, sustainable urban development very concrete we can talk about water management in the cities, waste management in the cities and energy management in the cities. Always having a sustainable approach, sustainable energy, sustainable water management and sustainable waste management so in brief that is what we do.
7	AS	So, are these projects in Malmö?
8	R5	We are regional in Skåne and in south Sweden you could say, Skåne, Blekinge and parts of Småland and Halland, so they are very often they have a regional approach but they could be local or national or international when we come to the Eu project some of them is international be-

		cause the money is designated for international collaboration interregional collaboration between Denmark, Sweden, Germany, Poland, Baltics states and so on.
9	AS	Have you implemented these projects or are they more in the pre phase?
10	R5	If there are any implementations?
11	AS	Yeah.
12	R5	We try to go for concrete projects where we do implement solutions for water management, waste management and so on so we yes, we have implementation projects where we call pilots, or test-beds or demos and so on. Some of them are not so concrete, they are implemented, we have a few international projects with the aim in helping our members or private companies for internationalisation, and export and in that case, it is not a technical implementation it is much more helping companies for export.
13	AS	So, you would say you work more with a sustainable city than a smart city?
14	R5	Up to now, yes, if you by smart mean some of digital approach, if that is what you mean with smart?
15	AS	Yes.
16	R5	So, digitalization is a buzzword and something that is coming and digitalization for sustainable human development is a very interesting topic coming up i guess, but we have not done that much yet.
17	AS	Can you give an example of these projects?
18	R5	What we do?
19	AS	Yes.
20	R5	One is called future it is about energy, its energy effective energy solution for the new energy and we have a project with Denmark, so we have seven cases in Denmark and south Sweden where we implement different kind of renewable energy project. In Malmö we have two cases in connected to the construction of Malmö sjukhus, or SUS Skåne university sjukhus where we have different smart energy solutions for the new built hospital, that kind of projects.
21	AS	So, if we should talk more about security, how do you work with security in these projects.
22	R5	I have to say it is not an issue that is discussed a lot, I have been here since some I have only been here at sustainable business hub since June/July last year. Security and personal security and anonymous and privacy it is not an issue that I can think of that I have heard actually.

23	AS	So, could that be that it is not so digital yet? So, you have not digitalization of it?
24	R5	It could be.
25	AS	And do you have plans to be more digitized later in these projects?
26	R5	I guess digitalization will be in our projects in the future.
27	AS	And do you think you will work with security issues then?
28	R5	Probably, in our case it is about digitalization links to how people are acting in the cities to some extent so there is privacy issue I guess in terms of, maybe in use of cameras, GPS, information that is linked to people's behavior and how people move in the city and what they do.
29	AS	I was thinking with the projects you mention with the energy, do you not use technologies, any type of technologies in those solutions?
30	R5	Technology is used but I have not heard about digitalization part of the technology it is more typical example using in energy is using waste heat from some kind of source, production some kind of waste heat in the process and then use that water, often there is water used in production and use that for heating buildings in the surroundings. That is a typical project. For example, in Lund. We have this Brunnshög development associated, located to the Max IV and ESS there is a project using the waste heat from the facilities from the experimental facilities to heating the Brunnshög area. And I guess there should be digital technology in the solutions, but I am not aware of it, I have not been.
31	AS	So, then it is not sensitive data that you collect.
32	R5	I don't think so, the sensitive data should be more when you start looking at how people behave in the city, how they move, what they do that could be sensitive. And behaviour is interest for mobility in the cities, I guess. Transportation, public transport, bicycle and for security reasons also. Before I was at Sustainable business hub, I was at a consultant called Thyrens and they had a project called security of safety people feeling secure of safe in certain areas of the cities. As soon you start looking at how people behave and how they move and you want to register, using cameras and devices I think it becomes an issue for privacy.
33	AS	And that is nothing you work with?
34	R5	Not yet. No, I don't know any of our projects where we come in contact.
35	A	Do you know if Malmö has any projects like that?
36	R5	I would guess that. Malmö stad, using cameras is something that is exploding isn't it, putting cameras all over the place.

37	AS	Do you have any technical solutions at Brunnshög, you do not see an issue if there should be a cyber attack?
38	R5	I guess it could be, because it is a vital infrastructure for the society for the cities in terms of energy and water. So, it could definitely be an issue.
39	AS	But you don't see that as a risk today?
40	R5	I don't know to be sure, I am not that much into the technical solutions, but if there is a cyber attack on energy solution or water solution, I guess it could be a risk.
41	AS	They might work with this in the projects, but you do not know?
42	R5	Yes, it should be the energy companies, in Lund it is Kraftringen.
43	AS	So, they are responsible for the security.
44	R5	Yes, they are responsible for the water management systems of the energy system when it is a municipal level with municipal responsibility. Then you have the fastigheter, the states of responsible for the municipal system, in Lund it is Kraftringen.
45	AS	And what is your responsibility, do you decide what should be done.
46	R5	We are often collaborating with other organizations, In Malmö it could be with Malmö stad it could be it is energy, Eon, Water issues could be with Va Syd then also with the private companies. So, it is always a number of organizations working together. And there is not very often we are the lead, another organization is in lead of the project and we are doing a part of it.
47	AS	Do you set agendas for security or something when you field these projects?
48	R5	Not really, security is not an issue actually.
49	AS	But why is it not an issue?
50	R5	I do not know. Because it is very technical, it is driven from technical, from needs of technical solutions water management problem or waste management problem and security is nothing that is brought up, it could be due to lack of competence maybe. There is not an issue that people bring out.
51	AS	In this project do you usually have education and training on what could happen if something goes wrong with security and maybe on security awareness or that?
52	R5	Not very much, or not at all honestly. It is very focused on solution and how can we have it implemented when we have this, new Brunnshög, low distribution heating, lågtempererad fjärrvärme in Swedish, very very

		interesting at the moment for energy people. So, it is very much on a technical implementation. They do not have security in mind, what I have heard about. So, it is quite interesting that you bring it up, because it is new to me.
53	AS	Yeah, that could might be because they are more focused on the functionality, and that it should help the city.
54	R5	Yes.
55	AS	The problem is then if there is a cyberattack is that happen.
56	R5	I have not heard about it, so it could be an interesting question for Kraftringen if we talk about Lund actually. They should have someone of course that is responsible of that kind of questions.
57	AS	An issue that we have identified is that there are so many different companies in the smart city and the sustainable city and that is also become a security issue because then it is easier to hack. If just one system is insecure that could like the entire city. Yes, if you have one weak link the system can like be hacked and that especially in the smart city because you get different companies to corporate. And they can have different standards on security.
58	R5	I described that we have a cluster we have a regional cluster connected to region Skåne, we have a bit of funding from region Skåne, we have nine clusters, cluster organizations. One of them is Mobile Heights.
59	AS	Yes, we have interviewed them.
60	R5	Yes, because they are very much into this, and they are having a collaboration project between the clusters on digitalization, how the different clusters will work with digitalization, but it is very new, it has just started. But I think digitalization will come much stronger in the future for us other clusters working with digital solutions in our daily work. But we will have this digital solutions implemented in our projects later.
61	AS	And then you will need the security?
62	R5	Yes of course.
63	AS	Yes, I think it will come maybe more common the security thinking when you use more digital parts.
64	R5	Yes, particularly we some cyberattacks and issues, security issues solutions we build up.
65	AS	So, if it should be a cyberattack at Kraftringen or Lund then there is not your responsibility?
66	R5	No, our projects are really at a pilot scale it is early innovation, so it is not implemented in further scale, so no I can't really see that should be

		an issue for security in that sense. What we do in our project is testing, demonstration and pilot.
67	AS	When you test, is there functionality you test and not security aspects?
68	R5	Yes, it is functionality aspects I would say. Then we work with other issues like business models. If we have this new interesting solution, then you also need to in the innovation process you need to develop your business model and how it should be delivered to the market. How it should be what kind of revenue streams. How to get paid for every solution that come with them and that kind of challenges that we are working with.
69	AS	Okay, it is interesting that you say that security is not an issue right now, but it could might be. And I wonder why it is like that, it is not the focus.
70	R5	It is not the first thing you think of, we have a lot of people very interested in their own technical area, they want to develop and innovate and come up with new solutions and implement it to the market, they do not have security on their mind, they have focus on the solution and that it can be implemented.
71	AS	It is like you want to have your product in the market fast. Yes, and then it might be security risks on that.
72	R5	Yes, that you do not think of.
73	AS	Yes, I think if attacks become more common people think about the security aspects more. I think that we in Sweden have not had so many attacks.
74	R5	No, we haven't heard of so many, there have been a few on the news I guess, but there is very little.
75	AS	Then it can be interesting for you to read our report.
76	R5	Yes, what we have heard is more the communication of radio and Tv and the internet of cost.
77	AS	Yes, because we have discussed a lot about solutions in Smart cities and they talk about technical solutions, or management solutions or legal solutions. Yes, policies and stuff like that. What they need to consider. And that is nothing you need to do now?
78	R5	No, it is not on the agenda for us at the moment until now. What did they say at Mobile Heights, they have a very different approach to digitalization than what we have.
79	AS	Yes, I understood it like they work with Future by Lund and just one year ago they decided to have a project with security to test the security and they work a lot with encryption and filter the data. Yes, I think they worked very closely with RISE also.

		But then they also mentioned that there are the companies that have a lot of responsibilities as you said with Eon. They need to have the security.
80	R5	Yes, and that also becomes a problem as I said that companies have different standards, so it is important to set that everyone in the city have the same policies or something.
81	AS	When you have these meetings with these companies, when you plan stuff, you do not plan for security for these, in the management solutions aspect?
82	R5	No, with my six- or eight-months experience here I have not heard of it to be honest.
83	AS	No okay that is very interesting. Do you want to add anything more?
84	R5	No, I don't think so, it was very interesting that you brought up the question and I will remember it and I will see what happens in the future. And I don't know what the direction the digitalization will have in our projects I am sure it will come. But that is also something that is quite difficult, if you are not involved in the digitalization, working with the technology it is a bit difficult to see what you can do with it, so you probably need some kind of cross interdisciplinary work so cluster like Mobile Heights will be a future collaboration for us.
85	AS	So, you need security aspects from someone else?
86	R5	Yes, and the digitalization knowledge, the competence, to implement digital solution into the smart cities. Have it integrated with the technical solutions and the challenges for waste and energy solutions.
87	AS	Thank you so much!

Appendix 7: Interview 6

Job position: Security coordinator Lund’s Municipality
Located in: Lund
Date: 2019-04-26
Type of interview: Face-to-face
Duration: 31 min

R6: Respondent 6
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	Then you can tell a little bit more about yourself and what you work with? *Men då kan du berätta lite mer om dig själv och vad du jobbar med?*
2	R6	Yes, my name is Lennart Larsson and I work as a security-provider at the municipality office. And at the department which is called “safety and security” and we are 4 people working there. It is someone who has the insurance department or the bite, someone who has emergency preparedness and someone who has civilian preparedness and so I am a bit in the middle. So I do a little of each. I work with emergency preparedness and safety work and that is everything from personal safety, in terms of choice security and event security in the municipality. *Ja, jag heter Lennart Larsson då och jobbar som säkerhetsanordnare på kommunkontoret. Och på den avdelningen som heter "trygghet och säkerhet" och vi är 4 stycken som arbetar där. Det är någon som har försäkringsavdelningen eller biten, någon som har krisberedskap och någon som har civilberedskap och så är jag lite mitt i mellan. Så jag gör lite utav varje. Jag jobbar med krisberedskap och säkerhetsarbete och det är allt från personsäkerhet, när det gäller valsäkerhet och evenemangsäkerhet i kommunen.*
3	AS	Mm.
4	R6	Then we have the “Valborg” soon when we should... Keep track of you. *Så vi har ju valborg nu strax som vi ska...hålla reda på er.*
5	AS & R6	*Laughter*
6	R6	But yes, and the risk and vulnerability analyse we do together with the administrations and do an overall which we submit to the county administrative board later. *Men, ja och risk- och sårbarhetsanalyserna gör vi ju tillsammans med förvaltningarna och gör en övergripande som vi lämnar in till länsstyrelsen sen.*
7	AS	Mm.

8	R6	And the rest, it's pretty much running-work. It is, yes, it is… something new comes up daily, it can be about person-safety, someone who is exposed to something or... And then keep on crime prevention too. So, I am the coordinator of the crime prevention council in the municipality. We meet the police and have regular meetings, every week we meet the emergency services, the police and yes, the security companies and a bit like that, field group to get an overview of how it looks in the municipality purely about safety. How it should be when it comes to crime and vandalism. Inserts action there. Mm. *Sen det andra, det är rätt så mycket löpande. Det är bland annat, ja det är... kommer upp dagligen någonting, det kan som sagt vara personsäkerhet, någon som blir utsatt för någonting eller... och sen hålla på med brottsförebyggande också. Så jag är samordnare för brottsförebyggande rådet i kommunen. Vi träffar polisen och har regelbundna möten, varje vecka träffar vi räddningstjänsten, polisen och ja vaktbolag och lite sånt där, fältgrupp för att få en överblick över hur det ser ut i kommunen rent säkerhetsmässigt. Så ska det vara när det gäller brott och skadegörelse. Sätter in åtgärder där. Mm.*
9	AS	Okay. I was thinking, have you been working with… Future by Lund sometimes have smart initiatives, have you joined them on their work then? *Jag tänker, har du varit med och jobbat liksom... Future by Lund har ibland smarta initiativ, har du varit med och jobbat?*
10	R6	We have participated on some of those meetings with Future by Lund, but we have not worked in some type of field group actually, we haven't done that. *Vi har varit med vid några sådana här möten med Future by Lund men vi har inte jobbat i någon arbetsgrupp direkt faktiskt, det har vi inte gjort.*
11	AS	What have you been doing then? *Vad har ni gjort då för något?*
12	R6	No, it has been when they have called, they call for meetings if it is one, twice a year or something like that, for the whole group. Where you tell what the workgroup has come up with or even ideas and thoughts. So, we have been involved in this, but we do not have workgroups were we actually work directly with them. It has, like, until now it hasn't been any work with them. *Nä det har varit när dom har kallat, dom kallar ju till möten om det är ett, två gånger om året eller något sånt, för hela gruppen liksom. Där man berättar, redovisar vad arbetsgruppen har kommit fram eller ja ideér överhuvudtaget och tankar. Så det har vi varit med på men vi har inte på arbetsgrupper, jobbat rent konkret med dom. Det har liksom, det har inte blivit så än iallafall.*
12.1	AS	What would you say are the biggest security issues for Lund as a city? *Vad skulle du anse är dom största säkerhetsproblemen i Lund som stad?*
12.2	R6	The biggest security issues are, I think it is the non-awareness of that risks do exist. People are really naive if you can say it like that. I work a lot with data

		and IT-security about how you handle your password and computers and stuff like that. I think that can be a big security risk. Then if anything should happen then it is, if there is a break in something, electricity supply or IT ... the infrastructure in it. So, we see that as the biggest threat. *De största säkerhetsproblemen är nog, det är nog okunskapen att det finns risker. Alltså folk är väldigt naiva om man får säga så. Jag jobbar jätte-mycket med data eller IT-säkerhet just för hur man handhar sina lösenord och datorer och sånt där. Så det kan jag tänka är en stor säkerhetsrisk. Sen så om det ska hända någonting så är det, om det blir avbrott i någonting, el-försörjning eller IT…infrastrukturen i det. Så det ser vi nog som det största hotet.*
13	AS	Have you had any cyberattack on any of your systems? *Har ni varit med om någon cyberattack på något av systemen?*
14	R6	We have not been affected in the municipality as we can say. People have certainly been trying or I know we had one attempt to infringe, but it has not become any greater of the least that has hit the business. *Vi har inte blivit drabbade i kommunen som vi kan säga. Vi har säkert fått försök eller jag vet att vi hade ett försök till intrång men det har inte blivit någonting större av det iallafall som har drabbat verksamheten.*
15	AS	Okay. How did you stop that then? *Okej. Hur stoppade ni det här då?*
16	R6	Oh, yes it is our IT department that goes in and looks, they see... So, I don't know this technical bit as I said. But they, they have firewalls and they have warning systems because if they see that it will come so they can shut down and so. Then you have the robustness, you have two servers from different... one, one scans off or scans of what has happened and puts it on the server every night and then it is back-up all the time. So, I think it's pretty safe, when they tell you they say it's pretty safe at least, but you don't know that until something happens. *Oj, ja det är ju vår IT-avdelning som går in och ser, dom ser ju.. alltså jag kan ju inte den här tekniska biten som sagt. Men dom, dom har ju brandväggar och dom har varningssystem för om dom ser att det kommer så dom kan släcka ned och så. Sen har man ju robusthet, man har två servrar från olika.. man, man skannar ju av eller skannar ju av vad som har hänt och lägger in på servern varje kväll och sen så är det back-up hela tiden. Så att jag tror det är rätt säkert men när dom berättar så säger dom att det är rätt så säkert iallafall men det vet man ju inte förrän det händer något.*
17	AS	I was thinking, what are the hardest challenges when it comes to security to tackle? *Jag tänker, vilka är dom svåraste utmaningarna när det gäller säkerhet att hantera?*

18	R6	Yes, the hardest is to create an awareness among the employees and citizens actually. It is probably what we work with most, as well as getting people to understand that one should perhaps be a little careful and even make back-ups on jobs you are doing and so. So that it is ... and not, do not surf on the net with the municipality's computers and pick up a lot of possible virus programs and things like that. *Ja, det svåraste är nog att skapa medvetenheten hos både anställda och medborgarna, faktiskt. Det är nog det vi brottas mest med, liksom att få folk till att förstå att man ska kanske vara lite försiktig och själv göra back-uper på arbeten man håller på med och så. Så att det är... och inte, inte surfa ute på nätet med kommunens datorer och plocka hem en massa möjliga virusprogram och sånt.*
19	AS	Mm. How do you work with this today? Do you have any education for the employees? *Hur arbetar ni med detta idag? Har ni någon utbildning för de anställda?*
20	R6	Yes, we do have it actually. We have one on the IT-department that works with, as I said, that informs about these regular, employee training or what to say. *Ja, det har vi faktiskt. Vi har en på IT-avdelningen som jobbar med det som jag sa som håller på och informerar om de här regelbundna, medarbetarutbildningar eller vad man ska säga.*
21	AS	Mm.
22	R6	But then it is, we can’t affect the citizens in that way. We can’t educate them. The employees are the case that we can focus on. *Men sen är det, vi kan ju inte påverka medborgarna på det viset. Vi kan ju inte utbilda dom. Utan det är ju dom anställda isåfall som vi kan inrikta oss på.*
23	AS	Do you think an education/training for the citizens will be necessary when more...? *Tror du det kommer behövas utbildning till medborgarna sen när fler…?*
24	R6	I think it will be. After all, we have a big, what to say, project ahead of us, that with heightened readiness. The municipalities have been commissioned to review civilian preparedness again and start building up. And this has been done with a bit of information, you have certainly seen around that you should be able to do 3 days and be prepared if the power goes and so on. After all, it is a way to create awareness for the public, but it will certainly be even more so in the future. *Jag tror ju att det kommer bli det. Vi har ju ett stort, vad ska man säga, projekt framför oss, det där med höjd beredskap. Kommunerna har ju fått uppdrag nu att vi ska se över den civila beredskapen igen och börja bygga upp. Och det har man ju gjort litegrann med information, ni har ju säkert sett dom här att man ska klara sig 3 dygn och vara beredd på om strömmen går och*

		sånt där. Det är ju ett sätt att skapa medvetenhet för allmänheten men det kommer säkert bli ännu mer så i framtiden.
25	AS	Mm.
26	R6	So, that is one way to do it. *Så det är väl ett sätt att göra det på.*
27	AS	Yes. Ehh, do you think security issues, and then I mostly think from an IT perspective can affect the privacy among the citizens? *Ja. Ehh, tror du sådana här säkerhetsproblem, och då tänker jag mest alltså från ett IT-perspektiv kan påverka asså "privacy" hos invånarna, alltså hur dom, alltså deras integritet?*
28	R6	Yes, it could go if there is someone who enters the system, you can get some information, of course. Then what to use them for, I don't know. *Ja det, det skulle det kunna gå om det är någon som kommer in i systemet så kan man ju få fram uppgifter, naturligtvis. Sen vad man ska använda dom till, det vet jag inte.*
29	AS	No. *Nej.*
30	R6	If you are a... Yes, I actually think there is a risk that it should be, someone should be able to enter the system in some way so... *Om man är en... Ja det tror jag faktiskt att det finns risk för att det ska kunna, någon ska kunna ta sig in i systemet på något vis så…*
31	AS	And how do you think this can affect all of the city systems that we use today and those that we will use in the future when we are more connected? *Och hur tror du det här kan påverka liksom alla stadens system som vi använder som vi typ, ja, kanske i framtiden också använder oss av när vi blir uppkopplade?*
32	R6	So it is, after all, we are extremely sensitive if something happens. If we were to get rid of the net for IT for a long time then we are right, very dependent of it, it is what I can say. There is much that will fail. I mean, you can't go shopping, you can't get your money out, you can't even ... So that, yes it will be a huge problem. *Alltså det är ju, vi är ju oerhört känsliga om det skulle hända någonting. Skulle vi bli av med alltså nätet för IT en längre tid så är vi rätt så, väldigt beroende av det kan jag säga. Det är mycket som kommer att fallera. Jag menar, du kan inte gå och handla, du kan inte få ut pengar, du kan inte ja... Så att det, ja det kommer bli ett jätteproblem.*

33	AS	Do you have any plans for if something like that would happen, that you have any…? *Har ni några, alltså har ni planer för ifall något sådant skulle hända, att ni har något...?*
34	R6	Yes, we have plans like… If, for example, we have the wage system that has been done, prepared so that one can pay out wages. *Ja, vi har ju planer på som... om, vi har till exempel lönesystemet har man ju liksom gjort, förberett så man kan betala ut löner.*
35	AS	Mm.
36	R6	And that is what you do with last month's and then you have to correct it afterwards and there are other seed things that do… I know that “vård och omsorg” has back-up for their patients and it is the same at “socialförvaltningen”. So, one has back-up besides too and even I know that “vård och omsorg” have in paper form too. So, one should, one can pick up if it would disappear quite a long time. *Och det gör man ju då med förra månadens och sen får man rätta till det i efterhand och det finns ju andra sådana där som gör på... Jag vet att vård och omsorg tillexempel har back-up med sina brukare och det är likadant på socialförvaltningen. Så man har back-up vid sidan om också och till och med vet jag att vård och omsorg har i pappersform också. Alltså det skulle man, man kan plocka fram om det skulle försvinna helt en längre tid.*
37	AS	How much responsibility would you say is on the municipality and how much is on companies, those companies that provides electricity and internet and so on? *Hur mycket ansvar skulle du säga ligger på kommunen och hur mycket ligger på företag, som såhär bidrar med el och internet och så?*
38	R6	It is like, we have contracts with all of them, both electricity and the telecommunications companies, but if it were to not happen properly, I do not know what those agreements are, so they cannot do anything either. *Alltså vi har, vi har ju avtal med alla, både el och telebolagen men om det skulle skita sig riktig så vet jag inte vad dom där avtalen, alltså dom kan ju inte göra någonting heller.*
39	AS	No. *Nej.*
40	R6	So that even if we have agreements that say that there should be no longer interruptions than that and so many minutes or hours or what you have now written so cannot... Even if it would be so you cannot do anything and then you sit there anyway. Then one can have how many contracts anyway so. The most important thing is to create a kind of redundancy that you have, that

		consciousness so you can build something alongside, if it should... if it didn't work. *Så att även om vi har avtal som säger att det inte får vara längre avbrott än så och så många minuter eller timmar eller vad man nu har skrivit så kan ju inte... även om det skulle bli det så kan man ju inte göra någonting, då sitter man ju där ändå ju. Så kan man ju ha hur många avtal som helst så. Det viktigaste är nog att skapa en slags redundans som man har, det medvetandet så man kan bygga upp någonting vid sidan om, om det skulle... om det inte skulle fungera.*
41	AS	We talked a bit about solutions as well, maybe we shouldn't go in so much on the technical ones? *Vi prata lite här om lösningar också, vi kanske inte ska gå in på dom tekniska jätte eller?*
42	R6	No that would be appreciated hahah. *Nej, det är tacksamt hahah.*
43	AS	Yes, but what do you have… what policies do you have when it comes to solutions? Do you have any in the municipality when it comes to security? *Ja, men har ni... vad har ni för policies när det gäller alltså lösningar? Har ni såhär på kommunen gällande säkerhet?*
44	R6	Like with back-up systems and redundancy? *Alltså med back-up system och redundans?*
45	AS	Mm.
46	R6	Oh, we have redundancy. First of all, we have... as I said, we, they are correcting all of the data-traffic every night and save on servers. And it is then two independent servers, and there is even one with cloud service too. So, the backup is there, after all, it never disappears, and it is available to pick up. But I do not know, how do you mean if we have done something else for prevention? *Aa, vi har ju redundans. Dels har vi ju... som jag sa, att vi, dem stämmer ju av all datatrafik varje kväll och sparar på servar. Och det är då två av varandra oberoende servrar och det finns till och med något som är molntjänst också. Så att den back-upen finns ju, det försvinner ju aldrig vad man säger utan den finns ju att plocka fram. Men jag vet inte, hur menar du med, om vi har gjort något annat för förebyggande?*
47	AS	No but we have been into it quite a lot on how you plan and stuff for security. But if you order one system, how do you think about security then? *Nä men vi har varit inne på det ganska mycket hur ni planerar och sånt inför säkerhet.* *Men om ni så här beställer ett system, hur tänker ni med säkerhet där?*

48	R6	So it is the procurement that gets to do... Yes, that it should, partly so it should be security classed, security protection. It is also this new security protection law that has come which you should look at and who, in particular, has access. Thus, they must be register-controlled and so, it is in the procurement. So, we have that with us all the time. But that is, I can say that it is very neglected in the municipalities. *Alltså det är ju upphandlingen som får göra... Ja att det ska, dels så ska det vara säkerhetsklassat, säkerhetsskydd. Det är ju också det här nya säkerhetsskyddslagen som har kommit som man måste titta på och vem, framförallt, som har tillgång. Alltså dom ska ju vara register-kontrollerade och sådär så, det finns ju med i upphandlingen. Så det har vi med oss hela tiden. Men det är, jag kan säga att det är väldigt eftersatt i kommunerna.*
49	AS	Okay. *Okej.*
50	R6	We have a great job with, starting to look at which key people have access to... And often it is so that it may not be the municipality's employees, but it is then another company that has another company so that it is a chain you have to follow up there. *Vi har ett jättejobb med, med att börja titta vilka nyckelpersoner som har tillgång till... Och ofta så är det så att det kanske inte är kommunens anställda utan det är då ett annat bolag som har ett annat bolag så att det är en kedja man måste följa upp där.*
51	AS	Yes. *Ja.*
52	R6	So that is, it's... We are not there yet but we are trying to clarify it so that for... visitors simply. So, people don't have what we don't know about having access to the systems. So, it is an important piece to work with. *Så det är, det är... Vi är inte där än men vi försöker att få klarhet i det så att vi för... besökare helt enkelt. Så att inte folk har som vi inte vet om har tillgång till systemen. Så det är en viktig bit att jobba med.*
53	AS	Who is it that will check this up? *Vem är det som kommer att kolla upp detta?*
54	R6	What did you say? *Vad sa du***?**
55	AS	Who is responsible to check up all the people? *Vems ansvar är det att kolla upp alla?*

56	R6	It's the security manager. In each municipality there must be a security manager. *Det är säkerhetsskyddschefen. I varje kommun ska det finnas en säkerhetsskyddschef.*
57	AS	Mm, okay.
58	R6	And it is the municipality director. But then she or he can delegate it so now it is the security manager who, in the municipality who is the security-protection manager as well. *Och det är kommundirektören. Men så kan hon eller han delegera ned det så nu är det säkerhetschefen som, i kommunen som är säkerhetsskyddschef tilllika.*
59	AS	Okay. I was thinking on another thing as well; do you evaluate these systems along time that they are still secure and so on? *Okej. Jag tänkte på det också, brukar ni utvärdera dom här systemen under tiden om de fortfarande är säkra och så?*
60	R6	Yes, in fact, it is now laid out so that it will be with regular, regularity, but that, it ... we are not there yet, nor can I say but we are looking at it so that we try to catch up. But then it is so that it is agreements that are written far back or further back in time that goes far ahead. And then you should go in and break them and that is… it's really hard. So, what we do now, we are looking at those we are now drawing instead, first and foremost, so one must take it along as the time passes. *Ja, faktiskt är det upplagt nu så att det kommer bli med kontinuerligt, regelbundenhet men det, det... vi är inte där ännu heller kan jag säga men vi håller på att titta på det så att vi försöker komma ikapp. Men, sen är det ju så att det är avtal som är skrivna långt tillbaka eller längre tillbaka i tiden som sträcker sig långt fram. Och då ska man gå in och bryta dom och det är.. det är jättesvårt. Så vad vi gör nu, vi tittar på dom som vi tecknar nu istället först och främst så får man ta det allt eftersom.*
61	AS	Mm. I was thinking if something happens, some attack against the security. Do you share information about this on the company or to the citizens about what is going on and…? *Mm. Jag tänker ifall någonting händer, någon attack mot säkerhet. Alltså brukar information delas då på företaget eller till invånarna om vad som händer mycket och…?*
62	R6	Yes, so... we have a crisis preparedness, a whole staff that we can get started, a crisis management staff. The municipal and there are communicators with on this also who have a communicator network that they are as well prepared for putting out information. And then it is down, it's really hard so. Then the question is, is it just in Lund or is it located in Malmö because we have an agreement or we have so we can reflect our website through Malmö example

		so we can get out in the same way also if it is only local here in Lund for example. So that is prepared, we have planned for it if there would be something like that too. But it's difficult, it's not easy. *Ja det... alltså vi har ju en krisberedskap, en hel stab som vi kan sätta igång, en krisledningsstab. Den kommunala och där finns ju kommunikatörer med också som har ett kommunikatörs-nätverk som dom är liksom förberedda på att lägga ut. Och sen ligger det nere, det är ju jättesvårt alltså. Då är ju frågan, ligger det bara i Lund eller ligger det i Malmö för vi har avtal eller vi har så vi kan spegla våran hemsida igenom Malmö till exempel så vi kan komma ut på det hållet också om det bara är lokalt här i Lund till exempel. Så det finns ju förberett, det har vi ju planerat för om det skulle bli något sånt också. Men det är svårt, det är inte lätt.*
63	AS & R6	*laughter*
64	R6	And this is precisely the case with communication to the citizens, how do you go out with information. It is very difficult and then it is the question of how much lies down. If there are only certain parts, you can go out on the radio, you can go out on TV for example or if that also down then it is... then it will be more with patches and then you have to run around and inform manually instead. *Och just det här med kommunikationen till medborgarna, hur går man ut med information. Det är jättesvårt och så är det frågan om hur mycket ligger nere. Är det bara vissa delar, kan man gå ut på radio, kan man gå ut på tv till exempel eller ligger det också nere så då är det ju... då blir det mer med lappar och då får man springa runt och informera manuellt istället.*
65	AS	Mm. I was thinking like when it comes to solutions for security and so on, which… what do you think are the most important ones if something happens? Or maybe, not only when something has happened but also if it is before something happens. *Mm. Jag tänker såhär liksom när det gäller lösningar mot säkerheten och så, vilka... vad anser du är det viktigaste att göra ifall något händer? Eller ifall, inte just kanske något händer också ifall det är innan också kan det vara.*
66	R6	Yes, that is... you get to look at those, we have society-important functions in the municipality that we have picked up. We do this in our risk- and vulnerability analysis. So, that they do, one must first of all make sure to cover or help so one has a robustness and it can be “vård och omsorg” that has patients who need a care all the time or medicine and stuff like that. So, it must work, so life and health go first to look at. Then you have to look at the other functions that must also work. *Ja, alltså det... man får ju titta på dom här, vi har ju samhällsviktiga funktioner i kommunen som vi har plockat fram. Det gör vi ju i vår risk- och sårbarhetsanalys. Så att dom, det får man ju i första hand se till att täcka eller hjälpa som man har en robusthet och det kan vara vård och omsorg som har brukare som behöver en vård hela tiden eller medicin och sånt där. Så det måste ju fungera, så liv och hälsa går ju först där att titta. Sen får man ju titta på det andra, funktioner som måste också fungera.*

67	AS	Mm.
68	R6	But we look at it a bit before that. We have something like, we have done something, a few years ago, called "styre-el" where you ... it is becoming more and more so that we use more power than we simply have, so right as it is so it may be that... or we are very close now that you should, you do not get as much power as you need. And then you have to pick, you have made a mapping of society-important functions in the municipality so that you can, like, yes, switch on power only in the hospital-area, for example. And then maybe you shut down some residential area that is not, it is important, but it is not as important as that ... you have prioritized it in different steps. So that, it is the same, the list of the society-important activities. We use it when we look at whether there would be anything else, for example everything from water pollution to ... you get to pick out these society-important pieces as well. And we have done that before and it is perhaps where you look at when something happens. *Men vi tittar ju litegrann på det innan så. Vi har någonting som, vi har gjort något, för något år sedan, som heter "styre-el" där man... det blir mer och mer så att vi använder mer ström än vad vi har helt enkelt så rätt som det är så kan det bli så att... eller vi är väldigt nära nu att man ska, man får inte så mycket ström som man behöver. Och då får man plocka, har man gjort en kartläggning av samhälls-viktiga funktioner i kommunen så man kan liksom, ja koppla på ström bara på lasarettets-området till exempel. Och så släcker man ned kanske något bostadsområde som inte är, det är viktigt men det är inte så viktigt som att.. man har prioriterat det i olika steg. Så att, det är likadant den, den listan med dom samhälls-viktiga verksamheterna. Den använder vi när vi tittar på om det skulle bli något annat, till exempel allt från vattenföroreningar till... så får man liksom plocka ut dom här samhälls-viktiga bitarna. Och det har vi gjort innan och det är kanske där man får titta på när det händer något sånt också.*
69	AS	Mm. What solutions take the most time and resources? *Mm. Vilka lösningar tar mest resurser och mest tid?*
70	R6	Everything takes a lot of time. But only to, as I talk about this with register checking staff for example. After all, it is a giant procedure, to check it out and it should be submitted to SÄPO because if you are going to check the registry so it takes a few days I can say before you get it back and so you should yes. So that, yes... I can imagine that all the preparatory work takes a lot of time and planning and what to do to be as safe as possible if something would happen. Then when that happens it will be another, then many will be involved but then you also have resources. We do not have such large resources now, before when we are in the planning stage. *Allting tar ju mycket tid. Men bara till att, som jag prata om det här med att registerkontrollera personal till exempel. Det är ju en jätteprocedur ju, att kolla upp det och det ska skickas in där till SÄPO för om man ska registerkontrollera så det tar ju några dagar kan jag säga innan man får tillbaka det och så ska man jaa. Så att det, ja.. jag kan tänka mig att det är allt förarbete tar jättemycket tid och planering och vad man ska göra för att bli så säker som möjligt om det skulle hända. Sen när det händer så blir det ju en annan,*

		då blir det många som blir involverade men då har man också med resurser. Vi har inte så stora resurser nu när det, innan i planeringsarbetet.
71	AS	No. I was thinking about when the city becomes more digital and so on. We have got the feeling that security is not the first priority? *Nej. Jag tänker på det när staden bli mer digital och sånt. Vi har fått den uppfattningen att säkerhet är kanske inte första prio, prioritet?*
72	R6	No, it has not been so I can say but it has become... the past few years the focus has become much-much more. When I started here on this unit 10 years ago it was a lot of emergency preparedness. You talked about it, but it has swung now so now is the security you are looking at. Everything from crime prevention to being safe when it comes to IT or that infrastructure there. So, it has become a lot more, but it could... it can be more, I can also think so. *Nej, det har inte varit det kan jag säga men det har blivit... dom senaste åren har fokus blivit mycket-mycket mer. När jag började här på denna enheten för 10 år sen är det nu då var det mycket krisberedskap. Man pratade om det men det har svängt nu så nu är det ju säkerhet man tittar på. Allt från brottsförebyggande till att det ska vara säkert när det gäller IT eller den infrastrukturen där. Så det, det har blivit mycket mer men det skulle kunna... det kan bli mer, det kan jag tycka också.*
73	AS	Because I am thinking, has it anything to do with that it takes a lot of time planning with resources and so on? *För jag tänker, kan det ha att göra med att det tar så mycket tid att göra förarbetet då med resurser och så?*
74	R6	Yes, it does, and we are becoming more and more people. We will hire more people just to look at these pieces as well. So that, yes. But as I said, we are a little bit in the back edge all the time and trying to catch up. *Ja, det gör det ju och vi blir mer och mer folk. Vi kommer och anställa mer folk just för att titta på de här bitarna också. Så att, ja. Men som sagt, vi ligger lite i bakkant hela tiden och försöker komma ikapp.*
75	AS	Mm, yes. You said that you are planning on hire more people for this part. Do you have any more future plans for handling the security? *Mm, ja. Du sa att ni planerar på att anställa fler inom just den här biten. Har ni några mer framtida planer för att hantera säkerhetsdelen?*
76	R6	Yes, yes indeed. We have done an investigation now for some year, last year that, made a new security program that will apply throughout the municipality. And it is now out for referrals among the administrations. It must be approved there first and then you should get it back. And if it goes through it will be a fairly big organizational change, you put more focus on the different businesses. That they should review that they are entitled to do some stuff. So that's it, yeah... *Ja, ja faktiskt. Vi har gjort en utredning nu för något år, förra året att, gjort ett nytt säkerhetsprogram som ska gälla i hela kommunen. Och det är ute på remiss nu bland förvaltningarna. Det ska ju godkännas där först och sen ska*

		man få tillbaka det. Och går det igenom så kommer det bli en rätt så stor organisationsförändring, man lägger mer fokus på dom olika verksamheterna. Att dom ska se över att dom har krav på sig att göra vissa grejer. Så att det är, jaa...
77	AS	You also mentioned this with Future by Lund, that you today are not so involved in their projects. Do you think this is something you will get more responsible with in the future? *Du nämnde även det här med Future by Lund att idag är ni inte riktigt involverade i deras projekt. Tror du det är någonting som ni kommer få ett större ansvar i senare?*
78	R6	Yes, I think we will. Make more time for that... the reason why we have not been so much with on it is that we do not have so much time over so we cannot participate. We already have a lot to do. *Ja, det tror jag att vi kommer göra. Få mer tid till att.. anledningen till att vi inte har varit med så mycket är att vi inte har så mycket tid över att vi kan inte vara med. Vi har fullt upp ändå.*
79	AS	Mm. Because it feels like they could benefit from your knowledge here? *Mm. För det känns som att dom kunde få ta mycket fördelar av er kunskap här?*
80	R6	Yes, and the other way as well. We could get ideas and knowledge from them, absolutely. Ja och tvärtom också. Att vi kunde få idéer och kunskap därifrån, så att absolut.
81	AS	Mm. If you would describe a bit if all the energy-supply would disappear or water, what would happen to the city according to you? *Mm. Om du skulle beskriva lite såhär om all elförsörjning skulle försvinna eller vatten, vad kommer faktiskt hända i staden då enligt dig?*
82	R6	Like, if someone takes control over… *Om någon typ tar kontroll kanske över...*
83	AS	Yes, or if it just disappears. *Ja eller om allt bara försvinner.*
84	RS	Yes, it's like I said. We have prepared with our crisis, that is, we have an organization if something happens. We have one, a law called "extraordinary" .... "the law of extraordinary events "where they have said that anyone who might, who came in 2006, where the municipalities should… just that they are entitled to do this risk- and vulnerability analysis, and there you should have a crisis plan for the municipality as .. and there we also have, and it is as well focused on, perhaps not specific events but more generally if it should go in. All the electricity, for example, disappears and such that all water disappears and something like that, so you have plans for how to do it. Then, we

		have a huge problem then, but we have a plan on how to do it, but yes, we do not hope it will happen. Because, that is... it is also that you focus on these society-important activities. You might get... you have to move people simply. Because it is an extraordinary event when everything, like everything, has gone to the barrel then you have a crisis management committee in the municipality. And it is KSAU really "kommunstyrelsens arbetsutskott" that sit there forming this. And they have the right to enter all the administrations and control, move staff and change finances and everything possible. So that then you can... we are quite many in the municipality, so we are almost 9000-10000 something that works. You might move people between the administrations, and you can… the urban construction office, for example, who are working on building permits may not have to have so many people then they can help on any other administration that needs staff. So that is, the planning is quite done but then it depends on what is happening, so you get to see. It is like the situation that may determine how to do it, but the plans are there, and it can be resolved in some way, at least. *Ja, det är som jag sa. Vi har ju förberett med våran kris, alltså vi har en organisation om det skulle hända någonting. Man... vi har ju en, en lag som heter "extraordinär.... "lagen om extraordinära händelser" där dom har sagt att alla som kanske, som kom 2006, där kommunerna ska… just att man har krav på sig att göra den här risk- och sårbarhetsanalysen. Och där ska man ha en krisplan för kommunen som... och där har vi ju också. Och den är ju liksom inriktad på, kanske inte specifika händelser men mer generellt om det skulle gå in. Alltså om all elen försvinner till exempel och sånt, att allt vatten försvinner och sånt. Så har man ju planer för hur man ska göra det. När risken försvinner, blir det någon IT-häveri, så då försvinner strömmen och så försvinner vatten, alltså allting. Och då, vi har ju jätteproblem då men vi har en plan hur vi ska göra men ja, vi hoppas inte det ska hända.* *För att, alltså det är.. också är det att man fokuserar på dom här samhällsviktiga verksamheterna. Man får kanske.. man får flytta folk helt enkelt. För är det en extraordinär händelse när allting liksom, allting har gått åt pipan då har man en krisledningsnämnd i kommunen. Och det är KSAU egentligen "kommunstyrelsens arbetsutskott" dom som sitter där bildar den här. Och dom har rätt att gå in i alla förvaltningarna och styra, flytta personal och ändra ekonomi och allt möjligt. Så att då kan man.. vi är ju rätt många i kommunen, så vi är nästan 9000-10000 någonting som jobbar. Man kanske flyttar folk mellan förvaltningarna och man kan.. stadsbyggnadskontoret till exempel, som håller på med bygglovshandlingar kanske inte behöver ha så många då utan dom kan hjälpa till på någon annan förvaltning som behöver, ja personal. Så att det är, den planeringen är liksom gjord men sen beror det ju på vad det är som händer så får man ju se. Det är liksom situationen som får avgöra hur man gör men planerna finns och det går att lösa på något vis, iallafall.*
85	AS	It feels like that even if there is an IT-attack that happens which affects that all electricity disappears, you have a plan for it. *Det känns som att även om det är en IT-attack som händer som påverkar att all el försvinner så då har ni ändå en plan för det.*

86	R6	Yes, we have, we have some sort of plan so we can get things going... the work so you get it on track. *Ja det har vi, någon form av plan har vi ju så vi kan liksom sätta igång och.. arbetet ändå så man får någon rull på det.*
87	AS	Yes. *Ja.*
89	R6	Then I know it's really hard. Now I know, did you hear about Höganäs who lost all mobile telephony, we could not talk to each other. It was an IT attack there. No, they drove down a pole, so it became, they became, they became like their own island. They have been here talking about it... it was really hard because you couldn't communicate with anything outside of it, you were in this little bubble but you didn't come outside of it. So that, it will be... and it was little Höganäs. If you think that it will be Skåne for example, then yes, that is a huge problem. But I think you can make the most of it. Then you do not know how much, Tetra Pak, what works on Tetra Pak when all IT... because it is so much that is controlled with it. So then maybe that whole factory is down at least, or the business. So yes, it will be a challenge I can say to sort that all out. *Sen vet jag att det är jättesvårt. Nu vet jag, hörde ni om Höganäs som tappade all mobiltelefoni, vi kunde inte prata med varandra. Det var väl en IT-attack där. Nej, de körde ned en stolpe så att det blev, dom blev, dom blev som en egen ö. Dom har varit och berättat om det.. att det var jättesvårt för man kunde inte kommunicera med någonting utanför, man kunde liksom vara i den här lilla bubblan men man kom inte ut utanför. Så att det, det blir ju.. och det var lilla Höganäs. Om man tänker sig att det blir Skåne till exempel så ja, det är jätteproblem. Men jag tror nog man kan få det mesta till att gå. Sen vet man ju inte hur mycket alltså, Tetra Pak, vad fungerar på Tetra Pak när all IT.. för det är så mycket som styrs med det ju. Så då kanske hela den fabriken ligger nere iallafall, eller verksamheten. Så ja, det blir en utmaning kan jag säga att reda ut allt det.*
90	AS	I am thinking like when you connect to when the trams are implemented and the trains and so on. What would that mean? *Jag tänker såhär när man kopplar typ till när spårvagnen är implementerad och tågen och sånt. Vad skulle det innebära?*
91	R6	Yes, yes you see it at the station today only when it is a signal error or something like that. After all, people do not come to their jobs or what they are going to do. It's really hard. *Ja, ja det ser man ju på stationen idag bara det är en signalfel eller något sånt. Det är ju, folk kommer ju inte till sina arbeten eller vad som ska göra. Det är ju jättesvårt.*
92	AS	Yes. You at least seem to have the right mindset, that you are planning a lot for… *Ja. Ni verkar ändå ha rätt tänk, att man planerar mycket inför...*

93	R6	Yes, we must do that, try. Then you cannot plan, you cannot imagine everything but you can at least try to see that... we have thought about the electricity disappearing, the water disappearing, what do we do and then you have this organization with, with crisis management staff who can then work from that. *Ja, det måste vi ju göra ju, försöka. Sen kan man ju inte planera, man kan ju inte tänka sig allt men man kan iallafall försöka se att... vi har tänkt om försvinner elen, försvinner vattnet, vad gör vi och sen har man då den här organisationen med, med krisledningsstab som kan jobba då utifrån det.*
94	AS	Do you have anything else to add that we have not talked about? *Har du något annat du vill tillägga som vi inte har pratat om?*
95	R6	No, but is sounds like an interesting master-thesis you are going to do. *Nej, men det låter som en intressant master-uppsats ni ska göra.*
96	AS	Yes, it is interesting. We have interviewed a lot of different people. You are our sixth person. *Ja, den är intressant. Vi har ändå intervjuat väldigt många olika personer som. Eller du är vår sjätte person.*
97	AS	We have interviewed 3 from Lund so it feels like we have a pretty good people of how you work with this now. *Vi har intervjuat 3 från Lund så det känns som vi har en ganska bra bild av ungefär hur ni jobbar med det nu.*
98	R6	Yes. *Ja.*
99	AS	Mm. You seem to think a bit more about security than many other cities, or that is the feeling we have gotten at least. *Mm. Ni verkar ändå tänka lite mer på säkerhet än många andra städer liksom, eller vad vi fått intryck av.*
100	R6	Yes, yes but that is good. We are trying at least. *Ja, ja men det var bra. Vi försöker iallafall.*
101	AS	Is it okay if we contact you if we have further questions? *Är det okej om vi kontaktar dig ifall vi har fler frågor?*
102	R6	Yes absolutely, that is fine. *Ja absolut, det går bra.*

103	AS	And I would love to read your paper when you are done with it. *Och gärna om ni när eran uppsats är färdig så skulle man gärna, jag vill gärna ta del av den.*
104	R6	Yes, absolutely. *Ja, absolut.*

Appendix 8: Interview 7

Job position: CIO Solna city
Located in: Stockholm
Date: 2019-04-29
Duration: 32 min
Language: English
Type of interview: Telephone voice call

R7: Respondent 7
AS: Amilia Åkesson &Sofia Gustafsson

Section	Person	Text
1	AS	Do you want to be anonymous in this study?
2	R7	Well, is everyone else anonymous or is it?
3	AS	Ohh, the other ones. We have have interviewed like 6 people before you and them that it is okay that they are not anonymous. But we will not like use your names so much, we just mention them.
4	R7	Yes, that's... it is okay. The same for me then.
5	AS	Okay. So, you can start tell a bit what you work with.
6	R7	Okay, I am the CIO of city of Solna and our IT is mainly rich outsourced, so my responsibilities are partly to manage the whole delivery from our service-providers. And then it is also to support the organization in digitalization and driving the IT and digital development in the city.
7	AS	Mm. Okay, I am thinking what is a Smart City according to you?
8	R7	A Smart City... That is a city where… I would say have a lot of automation. It can collect information about... things to make the city more efficient and more attractive for the citizens. Having an example, it could be better traffic planning, safer parks-lighting, and also a lot of about the services we are providing in school and elderly care.
9	AS	Mm. What Smart City initiatives or projects do you have in Solna or Stockholm that you work with?
10	R7	We have, one project within our elderly care, we work with RISE and some commercial parties, such thing as IoT and also evaluating effects of using IoT and personal integrity and legal aspects. And then we also have digital locks in our home care "hemtjänst".
11	AS	Mm.
12	R7	We have small number of march-weigh-built. And other ways I would say it is more to our external parties that we try to… requirements

		around smart real-estate management for instance or other things like that.
13	AS	Okay. How long time have you worked with Smart City projects or initiatives?
14	R7	Well, I have been in Solna for 2 years and I would say it is coming more and more for every year. So, the Vinnova project we have worked with since September last year. And we have had some small... with digital locks we have worked with for 3 years. It is taking quite a long time to implement.
15	AS	Mm. It sounds really interesting, both like with the digital locks and the health care and it is actually... our thesis is about security and privacy issues in Smart Cities and what do you think are the security issues with these Smart City initiatives that you have?
16	R7	Well, I would say in the health care, elderly care area, I mean it is both the security issues that you always have but there is a higher risk that IoT devices will be hacked or somehow compromised and then you will get access of a large part of the network or some systems. But then when it comes to healthcare it is also a lot about privacy and personal integrity. Questions "how we actually collect the data and what we do with it?" and just the feeling that you are being watched or on the surveillance, that's... I think that can be both... for some people it might be very positive, but others might feel uncomfortable with it.
17	AS	Mm. Have you had any like cyberattacks to these systems?
18	R7	Not to my knowledge, no.
19	AS	No, but if you have had... if you would had have any attacks and it would like affect different stakeholders that is in these systems. What do you think this would lead to?
20	R7	I would think that our end-users or customers would be more hesitant to accepting this kind of technology in the care and of course also for us in the city it would mean that we would be... Well, I would say we are very careful already but maybe it would be more difficult to test these technologies. And of course, I mean depending on what data it is, it could be a lot of other consequences if someone gets access to the data.
21	AS	Mm. I am thinking, what do you think are the biggest security issues? Because it is like, it could be different issues with the technology or other stuff but what technologies do you think pose the biggest security issues?
22	R7	What technology, well I think... I mean the different, anything that is connected to a gateway that you can somehow compromise. And especially if you would also get physical access to it and in somehow be able to get the data that runs through the gateway that way. I think that

		is one of the biggest risks, yes. And that you connect un-authorised devices to the networks, somehow if you can hack it.
23	AS	Yes. Do you think that there are any other issues than technology issues?
24	R7	Yes, I think... I mean the some of what I mentioned, the person integrity issue that being... that someone is either, somehow measuring, watching every step that you take and collect data about your movements or blood pressure or whatever. That is of course, can be negative for the person integrity.
25	AS	Yes of course, yes. Yes, that is a very big issue, especially when things are getting more connected and you use more IT or technologies. What do you think are the hardest issues to tackle when you work in these projects?
26	R7	So, I would say this, both from technology and more from an organization perspective or the people. Well first just getting acceptance for the technology and clusting it, I think that can be quite a big issue. And then also with our employees, some of them are not very used to technologies then they might not have the right education or the language skills, so it needs to be very easy for them. The actual software where they are receiving the data from the IoT devices needs to be intuitive, so that is also, the actual digital competence of our employees is a challenge that it is not high enough. And then it is more of technical issues and that we become more and more reliable both on the internet connectivity and of course electricity. So when things go down and if we reduce our, the number of people working there and we just have a lot of digital devices and IoT watching. Or instead of citizen care we have more of digital care, that of course becomes a risk which is something we need to find technical solutions for. So, that is why I think that is a challenge also.
27	AS	Yes of course. How do you think about privacy in the Smart City?
28	R7	Ehm yes, I think somehow as we start to collect more information that might be connected to an individual, we need to have a structure and a system for… I mean all according to GDPR, we need to be able to remove the data, we need to know what is connected to who and we need to be able to anonymize the data if we need this for like more overall. Yes, if we need the data but it can be anonymized then that is good and if it has to be personal then we need to be able to remove this and we need to be able to explain how we do this so that people feel safe in our environments.
29	AS	Do you have any solution or system for this today to handle this?
30	R7	No.
31	AS	Okay. So how do you think that privacy breaches can affect the Smart City systems?

32	R7	That I think, if there are any breaches then that would slow down the development and we need to focus in the more on security, I think. Which is, yes, I think this like challenge with sharing data, open data and then all the security risks. Of course, if we don't share data then it is smaller risks but then there is a value of the data. So, I think, really have good information models and follow that in the architecture when we build the IoT and Big Data environments. I think the keys are that we, the data that really needs to be protected so we protect that and the data that doesn't need that much protection can be shared and be open. Segmenting the data, I think that would be key in the future.
33	AS	Yes, you said in the future, so you are planning on doing this or do you do it now?
34	R7	I would say now we… well we don't… we haven't started collecting personal data yet.
35	AS	Okay.
36	R7	So, we are not really there yet. The things that we collect is not connected to individuals at the moment. And I wouldn't want to go there before we have a solution.
37	AS	No. So we have been in a bit about the security issues, like with all these Smart City initiatives. And now I want to know how do you work with like security solutions in the Smart Cities or how do you plan to work with it, or if like you have any technical solutions like firewalls and strong encryption and stuff like that?
38	R7	Well of course for our data connectivity we work with firewalls already. And anything that is on a server we also work with firewalls and also data encryption when we send something over the internet. When we precure solutions that are cloud based or such we put in our requirements, we have security requirements. And then I would also say that, I mean a part of the purpose of this Vinnova project we are doing is to develop better security for IoT devices and to develop a standard. So, I mean we are just a test environment, so we see that this is really important, that is why we want to be a part of a project like that. But I think what we can do is have multi requirements on our different IT vendors.
39	AS	Yes. Do you do any security test, like you mention that you had like different vendors and also other external collaborations. Like do you secure test things between you two so that everything is secure? The systems.
40	R7	Yes, that is something that we do.
41	AS	We also talked in our thesis about privacy by design and security by design. Is this anything that you work with?

42	R7	Yes, I would say since we have it in our IT architecture and in our requirements and it is something we consider every time we purchase or develop something together with our partners, yes.
43	AS	And also, do you have any education and training in your business or organization? Like you mentioned before that it is important that the staff have knowledge about different technologies, and do you have any education/training about security and stuff like that?
44	R7	Well, we are planning and will very soon have a general information security training for everyone that is new in the, in our organization. And of course, this is a first time for everyone.
45	AS	Yes, okay.
46	R7	Otherwise it has been more specific if you working in the specific area like the digital locks. They have a training on what those it means if, or around the procedures with the locks. Yes, so like specific groups have received training before everyone.
47	AS	Okay. What those this training like mean for everyone, what are they doing to learn more about security? Or what do you plan on this?
48	R7	No, we plan more general, to be aware of how we treat the information, or digital but also be aware that there are risk with certain kind of devices. So very high-level but also with some information, like where can you find more information and where are our issues or any questions. But high-level introduction to information security for everyone.
49	AS	Mm. Now you also mentioned that you didn't have had any like cyberattacks but if you…
50	R7	On my IoT devices you said.
51	AS	What?
52	R7	Yes, you asked on IoT devices.
53	AS	Yes, I asked before like if you had any cyberattacks, but you said that you didn't have anyone that you know of. But I was thinking if you would have any cybersecurity and privacy breaches in the organization, how would… like would you share this information with users?
54	R7	Depending on what it is, I might be able to share it with the MSB so. And with users, yes if anyone is… will follow GDPR so if it is personal data, some we have to inform everyone affected. And if it is not personal data just something else, we would inform the relevant parties.
55	AS	Yes. Do you have any plans in more ways how you would like to handle the cyberattack if it would happen?

56	R7	Well we have procedures together with our different IT partners and then of course if it is something bigger, we have our crisis management in the city.
57	AS	This crisis management, is it... are they from the municipality?
58	R7	Yes.
59	AS	I was also like thinking about management solutions and do you have like anyone in these, in your organization that works daily with like privacy and security issues and how to come up with solutions for this?
60	R7	We have an information security responsible and then we have IT security responsible that works daily with issues, so yes.
61	AS	Do you have any like organizational goals for the security in yes... do you have any specific goals like this is for everyone to take "ta del av" how do you say it?
62	R7	I think yes, that is part of why we also want to have this introduction training for everyone. Then we also, we have, we actually we have an overall information security policy which we are now updating with more specific guidelines for all our employees to be able to understand more of what it means to them.
63	AS	Mm, okay. Do you have anyone that is like completely responsible for the Smart City security or the smart initiative security?
64	R7	No, not specifically for Smart City or smart initiative, no. Just overall IT security.
65	AS	Okay. So, we have talked about, or we are writing about like different solutions and we have talked about different solutions. But do you think that there are any solutions that are any more that are more important than anyone else because it is like you can have digital solutions, technical solutions with good firewalls and encryption. And you can also have like management solutions and how you plan for how to tackle the security issues. But do you think that any solution is more important?
66	R7	I would say that it is, if the users don't know how to use the technology it doesn't matter what other kinds of security you have because then you will always have security breaches so, that is definitely important. And also, to know what to do when you have a breach.
67	AS	Yes, so you are prepared for if something happens?
68	R7	Yes.
69	AS	So it is maybe more like, it is important to educate and train people so they are aware of the risks associated with...
70	R7	Yes.

71	AS	What solutions do you think takes most time and resources?
72	R7	That might be the one to educate people because there are a lot of people to educate.
73	AS	Mm, okay. Do you have any like specific solution for the privacy issues, you mention like that you, when you collect a lot of data and… but do you have any plan or implementing solutions for this or do you have it already?
74	R7	No, not any practical solution that I can describe but it is more about getting the consent and awareness from the accurate costumer or users and their relatives.
75	AS	Mm.
76	R7	So maybe some education and awareness, there is one. Otherwise I mean, the more technical solutions are to have the, that we need to, as we develop or build this we need to have a good information structure so we know exactly where we have which data.
77	AS	Yes. Do you have any other future plans for how to handle the security and privacy issues?
78	R7	Not that I can think of, I mean and then we of course have a strategy that you need to have identification and also authentication and all of that, of course. But that is not something that is new so no I wouldn't say that we have anything else that I can mention now.
79	AS	Mm. Do you have any other security solutions that we have not talked about yet that you want to mention?
80	R7	No, it is only our identification and authentication management and how we work with like the authentications and what kind of "behörigheter". So, it is more that area, to make sure that only the necessary people have access.
81	AS	Okay so it is about who has access to different…?
82	R7	Yes, access.
83	AS	Okay. Do you have anything else that you want to add that we have not talked about in this interview?
84	RS	No, not that I can think of now, no.
85	AS	Okay. Is it okay for us to contact you if we have any further questions?
86	R7	Sure, no problem.
87	AS	Thank you so much!

Appendix 9: Interview 8

Job position: Smart City and digitizing consult
Located in: Frederiksberg/Copenhagen
Date: 2019-05-03
Duration: 35 min
Language: English
Type of interview: Skype voice call

R8: Respondent 8
AS: Amilia Åkesson & Sofia Gustafsson

Section	Person	Text
1	AS	We would like to start, if it is okay that we record the interview?
2	R8	Yes that is okay.
3	AS	And do you want to be anonymous in the interview?
4	R8	It depends what we are talking about.
5	AS	Yes you can decide that afterwards. We will not write your name but we will maybe write your position if that is okay for you?
6	R8	Yes that is okay.
7	AS	Okay great. So would you like to start tell us what do you work with?
8	R8	I work with coordinating and implementing some of the Smart City solutions that we are implementing in the city of Frederiksberg, I am sitting in a central office if you say so for our technical and our environmental department. And our focus on Smart City is mainly on these topics if you can say so, regards to climate, mobility and so forth. Environmental issues.
9	AS	Okay. And what is a Smart City according to you?
10	R8	That is a good definition, changed a lot during the last couple of the years. I would say it is about mostly having the right decision material in, it is about engaging people in the right sense and having the right data to actually divide engagement and the right decisions in the city. So that would be for sense if we talk about traffic, it is about giving insight about how the city use so we can make the right from proper planning for the city, and in that sense understanding the citizen's needs, the citizens needs and so forth. So, it is a big mixture of data, technology and user perspective.
11	AS	Okay yeah. And how long time have you worked with Smart Cities?

12	R8	Me personally have working with it since we started working on a strategy for our city so that has been since 2014.
13	AS	Okay and what kind of Smart City initiatives do you have in Frederiksberg or Copenhagen?
14	R8	Frederiksberg is a small entity within the city of Copenhagen, so we have our own infrastructure and our own Smart City budget. The most important Smart City initiative which is already fully implemented and full scale is our Smart City network which is a digital infrastructure that actually test our Smart city solutions. So, we have a full scale Wi-Fi system, we have Laura-network, we have fiber-network, electricity to actually put on all the gadgets that we need in the center that we need to monitor or yeah data or responses in the city. That is the first informational important project that we have implemented. Then we have something called parking which is a project that focus on how to optimize the parking spaces in the city but also how to guide car owners to the right or fastest to the first available spot, nearest available spot to their end position.
15	AS	Mm.
16	R8	We have several climate solutions, which are climate application solutions in general but where we are implementing Smart City elements in to it. To first of all to register and monitor how the flow water is in periods where we expect peaks of water. But also, to test if our solutions are actual giving the result that we want. And also, to actually regulate the flow water in the city. This is something that we are working on right now. And that we have some other small projects here and there but mostly within the themes of traffic, mobility and climate that is our main focus right now.
17	AS	Okay, so you have some initiatives that are already implemented, and some that you are working with like projects?
18	R8	Yeah. I would say Smart City projects will, yeah they are never already implemented because you always get wiser and then you put a new element or a new level on top of it, so we do have full scale projects which are no longer pilot projects but which are implemented. But we also have some that are which are just proof concepts projects which we are testing out because technology is so new or our knowledge how to use the technology is so new, so we need to gain more insight about that.
19	AS	Okay. So, our thesis is about security challenges and how you work with these in the Smart City. So, what kind of security challenges do you have in your Smart City?
20	R8	First of all, we need to understand if there is any personal data involved. That is one of the biggest issues right now due to the law GDPR implementation last year. And so that is one of our foremost priorities when we are looking into security. It is a Smart City project that in any sense handle personal data. Then we have all infrastructure about security, can you hack in to the data or misuse something else,

		even if it is not personal into it. Can you change utility or water or change blockage in the city or somehow, yeah misuse the data in a sense that is not invented. So that on the technical gadget. Security built into the sensors, into the network infrastructure but also into the data in three levels, and of course the user perspective.
21	AS	What would you say are the biggest issues for the security in the Smart City?
22	R8	Lack of knowledge about security.
23	AS	Okay is it the lack of knowledge from the citizens, or from the employees?
24	R8	Both actually of course the employees know that you need to have a lot of insight about this but they don't necessarily know, they are not 100% knowledgeable about security issues and all Smart City solutions so we always ally ourselves with experts within our own organisation but sometimes also externally. The lack of knowledge is something just to acknowledging that I am not, knowledgeable enough about security on this gadget that I need to go somewhere external and get more information. And for the citizen part yes a lot, we do get some kind, some contact from the citizens that are concerned about what we use data for, if they in somehow are vulnerable to the projects that we implement but there is not that many, but it is something that happens but it is not as bad as I feared actually. Does that make sense?
25	AS	Yes absolutely. Do you work anything with training or education for the citizens or the employees?
26	R8	Not in training per se but I do have projects where I am and dialoguing with my colleagues or with citizens, I do for instance a Smart City challenge a hackathon. I am part of, I have been for some time now. So I do not mean what you mean with this question if are educating citizens, can you elaborate?
27	AS	Yes, if you educate the citizens about the security risks when they are involved in the Smart City applications.
28	R8	It is not my role to educate them, my role is to consult them or advise them to look into security issues and get expert contact or collaboration partners something like that.
29	AS	Okay, yeah. And do you share information to the citizens about what the data is used for in the Smart City?
30	R8	Mm yeah, actually if I could start just a step back. I think it is more important to actually tell what parts of GDPR and you always have to explain what the purpose is when gathering the data. And when you tell what the purpose is then you sometimes also get the sense why this is important and then it is easier to explain the security part of it or not. So, I always, I always start by explaining the purpose of things and then we take it from there.

31	AS	Yeah, okay. That sounds good. Have you had any cyberattacks against the Smart City systems yet?
32	R8	Mm not to my knowledge no. But that is also a difficult question because the infrastructure for instance is not us who are the owners of it, that is the utility companies but we are during a secure line. If happen any cyber-attacks that would probably be on the utility company but we haven't been told about it. But I don't think it has happened.
33	AS	Okay.
34	R8	But we do not have any incidents right now that we are aware of. But we do have sensors and gateways and stuff like that which we have had ideas about being not secure enough which in that sense that we have a collaboration with the university and they have a hackalab that we use a lot to try to fix some of the issues that we think that might be.
35	AS	And how do think about privacy in the Smart City?
36	R8	I think privacy is important, to understand and to, yeah.
37	AS	And what are the challenges to the privacy.
38	R8	I think the biggest challenge is, yeah that is a good question. I think it is being aware of it when you actually breaching it, when you are going too far. There are some privacy issues which are regulated by the law. Which are beyond the GDPR if you say so which is for instance if you have some issue or problem with the municipality then GDPR apply. But there can be a privacy issue which you are allowed to do something with the data. Then we are talking a lot about private data here. I think that is very important that you have an understanding when you go too far as a private person. The Smart City solution as we understand it, they are barely, in what we use anyway in the municipality of Frederiksberg where we started. Barely use private data. We are always alert and know that we don't mix data which can end up being traceable to persons, but we rarely use private data, for me to say.
39	AS	So, you just have private data in some projects?
40	R8	So far, we have not had any private data in any of our Smart City projects.
41	AS	Okay.
42	R8	But that is not the same, if you start for instance tracking movement, we should be aware that this data can be used as a piece of privacy data. So, we are very much aware about some of the issues that can be with using data, which for say is not private from the beginning but which can be private. When together with other data.
43	AS	Okay, what are the issues you see here?
44	R8	The same issues when you privacy in general that you can misuse, you can hack them, you can do evil in a lack of better English word right

		now. Yeah you can do something to benefit your own position that is not something that we are trying to promote in any way.
45	AS	Okay. We have also had a question about how do you think privacy breaches can affect the Smart City system. What do you say about that?
46	R8	First of all if its public humiliation because people will be very against implementing more Smart City solutions first of all. Regards of a couple of things I have already mentioned I think, privacy issues will be a part of Smart City solutions. In the future. But this is something we decided not to focus on right now. Because the knowledge so far in the municipalities are so far, we still to navigate in GDPR, and with all these technologies and so forth. So, we start focusing on if you say to not vulnerable. Some of the problems that can be solved without privacy issues. In my department. There are other departments perhaps that are experiencing or implementing projects which are more use of privacy data. But then it is not defined as a Smart City project it could just be a project or health project.
47	AS	Okay yeah. Our thesis is also about how you work with the solutions to the security and privacy challenges in the Smart City. And how do you work with security and privacy within the Smart City initiatives that you have?
48	R8	I think I have answered it already, but I am not sure if you need more.
49	AS	Yes, something more would be great.
50	R8	First of all, there are some rules for what you have to do. We are fully applied or trying at least to try to be fully applied to GDPR as possible. So, we do all we can in the project to document the setup and all the things we have to do. Then of course we implement all the security guards we can in the hardware, the software and measures around that. I would say we are used to work with data and personal data in the municipality, so this has not changed just because it is a Smart City project, but again the most of our Smart City projects are primarily not the private data. So yeah.
51	AS	Okay, so you talked about that you have some legal solutions, do you have any technical solutions to make sure that the Smart City initiatives are safe?
52	R8	Yes of course.
53	AS	And what kind of technical solutions?
54	R8	We have well, I am not sure I can go into details with of all of it. But of course, we think about how we do the setup, so we do have protection, hardware protection that, when we have sensors in the street, we try to protect them with the hardware. The way they are built. So, the chips or the data is not accessible by breaking into the boxes or the sensors. We do have some time of monitor on some of our sensors. We

		have software protections as well in different sensors as well. We have malware protection and firewalls things like that. We have people watching over the data packages.
55	AS	Yes Okay. What solutions would you say are the most important ones?
56	R8	In security systems?
57	AS	Yes, in all kind of solutions, management, legal or technical solutions. Which ones are the most important ones to make sure like the smart city system is secure and safe?
58	R8	I would say that all together is important not one alone. I think that is very important, you can never look at things isolated always, if you implement some kind of system then you also suppose, you have to see it in collaboration. One does not go alone.
59	AS	Do you have a security team or someone that is responsible for the security in the Smart City?
60	R8	The utility company does yeah.
61	AS	Is it like a team or is it just one person?
62	R8	I am not actually sure, I would suppose it is a team because they have 24h of surveillance.
63	AS	Okay, so if something happens in the Smart City, then they would start working with... yeah?
64	R8	Yes. But we have to once again go back to what kind of projects are we talking about because if it is life critical systems of course you will have to have a bigger response unit, try to go in and fix some of these stuff. The worst case scenarios that would be in our situation would be for instance that you could not get measurements from the utility companies or from the heat measure and that is not a world risk if you say so. You do not need to have a response in 30 minutes of 10 minutes or in 5 minutes. But they do have security personal.
65	AS	Okay. I think you mentioned something about this in the beginning, but do you identify what kind of security challenges you have before you start with the projects?
66	R8	Yes. That is part of the whole GDPR process. We go through what king of known risks that we know if it’s one kind hacking from another or if it is yeah. The liberate what's called the leaking information we always go through that especially when it is personal data.
67	AS	Okay and do you work with privacy by design or security by design in the projects?
68	R8	Yes.

69	AS	And, how do you?
70	R8	If first of all identify if we need private data for instance, and if we do that we try to think where we can minimize the access of private data. But again, most solutions are not handling private data but that is also privacy by design. So, or security by design in some sense. So that is something that we do think of into our solutions yes.
71	AS	Okay great. And do you have any goals for the security in the projects?
72	R8	As a defined goal?
73	AS	Yes.
74	R8	No, we don't. This is a goal in itself to secure that but that is the data is secure but also that we have secure seat of data is also an issue. But nothing more specific than that no.
75	AS	Okay and what solutions would you say take the most time and resources to work with in the security perspective.
76	R8	I would say right now that it is camera technology working with data there. That is new ground for us so that is something we try to understand and figure out how to use in the right way.
77	AS	And why is that the ones that takes the most time?
78	R8	Because there can be a breach and if it is a number of camera feed of pictures there would be able to identify persons and that is something that we are designing data for not trying to do so we are thinking very much about in edge computing and trying to eliminate as much of personal data as possible so we just get the feed of counting of people and not necessary who it is.
79	AS	So would you say that you evaluate the things you know that take the most time and most resources and gives that the most time and resources to make sure that is safe, like if we compare the cameras to something else that you know that the camera will, yeah it is hard to describe what I want to ask.
80	R8	Yes but I also think we get wiser every time, of course we allocate many resources when something is new and we have to figure out when to use it, but then we gain some knowledge and the knowledge is not notice, you can use it that project but it is another project. So I think it is a learning curve, we gain knowledge all the time, as new levels about what we already know, but the same people are working more or less as a central unit and advising our colleagues that are maybe new in some projects so we help each other in that sense.
81	AS	Do you work anything with testing when you have new technologies?
82	R8	Yes.

83	AS	And how do you work with the testing?
84	RS	Hm, in a new system where we try to get knowledge about the data, how the come and test the data with the people who are actually supposed to understand the data. Give that the right sense of meaning for them or do we have to adjust the type data that comes into it. It is not just the driven but also the usage of the data. So, we are back in the purpose when we are doing the project. Security wise we also test the data, do we have the right setup.
85	AS	Do you have a specific test environment you do this in?
86	R8	No.
87	AS	Do you do it in the city when it is already implemented?
89	R8	Yes we don't have a living lab or a test lab, we do have participation with the two Skylab and hackalab and other places if we need to go and test some hardware but we do a lot of live testing in the city but then we do it as a part of a pilot project or a proof concept and the we scale that up when we have the right setup.
90	AS	Okay, and if you found that something is wrong from the security perspective, how should you tackle that?
91	R8	We are just, we aboard. If you found any breaches or something, then we of course just or we stop the project, so the data is not transmitted.
92	AS	I just have one more question, that we talked a little bit about before but how do you think the security can affect the privacy of the citizens.
93	R8	That was what we were talking about, there are several levels to that question, if you think of it as a more theoretical question or you know, question of course this would be, the perspective of a Smart City, of what you can do can be a potential privacy disaster if you are a privacy lover. There is no doubt about that. But I am not sure we are ever going to go that far. Because we have all these regulations, and laws and personal interest, what do we want to use the data for. And if the data does not give meaning in itself or the usage of the data give meaning then you wont start collect the data. This is very much connected with the resources and the money we have to put into the project so we as a public sector would never implement anything that hasn't had any kind of legal purpose.
94	AS	Okay.
95	R8	I am fully aware that there will be other entities that will be able to gain from the data and use it in, private sector. You have all the cases with Google and so forth and you know that, you are more about how privacy issues are there. As a public sector we are much more regulated so I think that will be my take from that.

96	AS	Okay, great.
97	R8	Does it make sense, it is very difficult for me to explain.
98	AS	No that makes sense absolutely. I was also thinking about the collaboration between you as a public sector and the private company how much responsibility in the security aspect are on the private companies that you use the technologies from?
99	R8	Yeah that is a long road, but it is very clearly specified in the GDPR as the data handler, even though I am not the primarily one but the other ones have the same rules that they have to live, or have to fulfill. I forgot the question what did you say?
100	AS	Yes, let's say if you implement something from a private company, some kind of technology, do you evaluate the technology before you implement it, or how does that work?
101	R8	Then you focus on the technology, you are not focusing on the data?
102	AS	No more from the technology, like if it is secure.
103	R8	Okay but then we do evaluate it yeah.
104	AS	Okay great. Do you want to add something more that we have not talked about?
105	R8	Hm, I think it is very important when you are talking about Smart City solutions, because I understand you have very much privacy agenda and I think it is very much, we are very alert, but that most Smart City solutions don't actually handle personal data. They do when you get into the field of healthcare and stuff like that, then we are a totally different level and then you would call it smart city citizens or the terms and I know the term Smart City is very broadly used nowadays, and I think that it is very important to have that focus on what's, why you ask me what my definition of a Smart City is of course. We use it differently in different parts in the public sector but also in the private sector. And if you go to my colleagues in the health department, they wouldn't say they do Smart city solutions they would say they do smart health as I said before. They would more call its digitalization. So, it is the same issues anyway. Security is an issue, never the less so, something we always have to look into and be aware of.
106	AS	Yeah. Great. Thank you so much it was very interesting.
107	R8	You are welcome.
108	AS	Is it okay for us to contact you if we have any further questions?
109	R8	Yes of course that is fine.

110	AS	And yes, back to the question do you want to be anonymous in the study?
111	R8	No that is fine. You can put my name.
112	AS	Okay, thank you so much.

References

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I., & Airaksinen, M. (2017). What are the differences between sustainable and smart cities? *Cities*, *60*, 234–245. https://doi.org/10.1016/j.cities.2016.09.009

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, *22*(1), 3–21.

Aldairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, *109*(2016), 1086–1091. https://doi.org/10.1016/j.procs.2017.05.391

Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., … Sansurooah, K. (2017). Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*, *22*, 3–13.

Bakıcı, T., Almirall, E., & Wareham, J. (2013). A smart city initiative: the case of Barcelona. *Journal of the Knowledge Economy*, *4*(2), 135–148.

Benevolo, C., Dameri, R. P., & D’Auria, B. (2016). Smart mobility in smart city. In *Empowering Organizations* (pp. 13–28). Springer.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. https://doi.org/10.1108/IntR-01-2014-0020

Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 1392–1393. IEEE.

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499–507.

Brinkmann, S., & Kvale, S. (2005). Confronting the ethics of qualitative research. *Journal of Constructivist Psychology*, *18*(2), 157–181.

Cocchia, A. (2014). Smart and digital city: A systematic literature review. In *Smart city* (pp. 13–43). Springer.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access*, *6*, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Demirkan, H., Bess, C., Spohrer, J., Rayes, A., Allen, D., & Moghaddam, Y. (2015). Innovations with Smart Service Systems: Analytics, Big Data, Cognitive Assistance, and the Internet of Everything. *CAIS*, *37*, 35.

Docherty, I., Marsden, G., & Anable, J. (2018). The governance of smart mobility. *Transportation Research Part A: Policy and Practice*, *115*, 114–125.

Dorasamy, M., Haw, S.-C., & Vigian, T. (2017). Cyber Security Violation in I0T-Enabled Bright Society: A Proposed Framework. *PACIS*, 244.

Edwards, L. (2017). Privacy, Security and Data Protection in Smart Cities: *European Data Protection Law Review*, *2*(1), 28–58. https://doi.org/10.21552/edpl/2016/1/6

Elmaghraby, Adel S, & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, *5*(4), 491–497.

Elmaghraby, Adel Said. (2014). Security and Privacy in the Smart City. *Proceeding of 6th Ajman International Urban Planning Conference AIUPC6: “City and Security,”* (March 2013).

French, A. M., & Shim, J. P. (2016). The Digital Revolution: Internet of Things, 5G, and Beyond. *CAIS*, *38*, 40.

Future by Lund. (2019a). Smart offentliga miljöer. Retrieved May 28, 2019, from http://futurebylund.se/project/smarta-offentliga-miljoer

Future by Lund. (2019b). Våra projekt. Retrieved May 24, 2019, from http://futurebylund.se/projekt

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *Bdj*, *204*, 291. Retrieved from https://doi.org/10.1038/bdj.2008.192

Goel, S. (2015). Anonymity vs. security: The right balance for the smart grid. *CAI*S, 36, 2.

Harbers, M., Bargh, M., Pool, R., Van Berkel, J., Van den Braak, S., & Choenni, S. (2018). A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges. *Proceedings of the 51st Hawaii International Conference on System Sciences*, (January). https://doi.org/10.24251/hicss.2018.278

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 464–467. IEEE.

Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *International Journal of Advanced Computer Science and Applications*, *7*(2). https://doi.org/10.14569/IJACSA.2016.070277

International Telecommunication Union. (2008). *Series X: Data Networks, Open System, Communications and Security*. Retrieved from file:///C:/Users/JorgeEnrique/Downloads/T-REC-X.1084-200805-I!!PDF-E.pdf

International Telecommunication Union. (2017). Global Cybersecurity Agenda (GCA). *International Telecommunication Union (ITU)*. Retrieved from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Järvinen, P. (2008). Mapping research questions to research methods. *IFIP World Computer Congress, TC 8*, 29–41. Springer.

Jokar, P., Arianpoo, N., & Leung, V. C. M. (2016). A survey on security issues in smart grids. *Security and Communication Networks*, *9*(3), 262–273.

Kajtazi, M., Vogel, B., Bugeja, J., & Varshney, R. (2018). *State-of-the-Art in Security Thinking for IoT*. 1–15.

Karyda, M., & Mitrou, L. (2016). Data Breach Notification : Issues and Challenges for Security Management. *Mediterranean Conference on Information Systems (MCIS).*

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, *9*(3), 2012–2052.

Khatoun, R., & Zeadally, S. (2016). Smart cities: concepts, architectures, research opportunities. *Commun. Acm*, *59*(8), 46–57.

Khatoun, R., & Zeadally, S. (2017). Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), 51–59. https://doi.org/10.1109/MCOM.2017.1600297CM

Kitchin, R. (2016). *Getting Smarter About Smart Cities: Improving Data Privacy and Data Security*. (January), 82.

Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. *Journal of Urban Technology*, *26*(2), 47–65.

Kvale, S. (1996). The 1,000-page question. *Qualitative Inquiry*, *2*(3), 275–284. https://doi.org/10.1177/107780049600200302

Landahl, G. (2017). *Smart & Connected*. 16. Retrieved from http://international.stockholm.se/globalassets/ovriga-bilder-och-filer/smart-city/brochure-smart-and-connected.pdf

Lee, J., Kim, J., & Seo, J. (2019). Cyber attack scenarios on smart city and their ripple effects. *2019 International Conference on Platform Technology and Service (PlatCon),* 1–5. IEEE.

Li, Jin, D., Hannon, C., Shahidehpour, M., & Wang, J. (2016). Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Physical Systems: Theory & Applications*, *1*(1), 60–69.

Li, Y., Dai, W., Ming, Z., & Qiu, M. (2015). Privacy protection for preventing data over-collection in smart city. *IEEE Transactions on Computers*, *65*(5), 1339–1350.

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199.

Manville, C., Cochrane, G., Cave, J., Millard, J., Pederson, J. K., Thaarup, R. K., … Kotterink, B. (2014). *Mapping smart cities in the EU*.

Marsal-Llacuna, M.-L., Colomer-Llinàs, J., & Meléndez-Frigola, J. (2015). Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative. *Technological Forecasting and Social Change*, *90*, 611–622.

McLaughlin, M.-D., & Gogan, J. (2018). Challenges and Best Practices in Information Security Management. *Mis Quarterly Executive*, *17*(3), 237–262. Retrieved from https://www.isaca.org/cyber/

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Negre, E., Rosenthal-Sabroux, C., & Gascó-Hernández, M. (2017). Smart Cities, Smart Government, and Smart Governance Minitrack (Introduction. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 2792–2793. https://doi.org/10.24251/hicss.2017.337

Nikander, P. (2008). Working with transcripts and translated data. *Qualitative Research in Psychology*, *5*(3), 225–231.

Owens, W., Dam, K., & Lin, H. (2009). Technology, law, and ethics regarding US acquisition of cyberattack capabilities. *Washington, DC: National Research Council of the National Academies of Science*.

Pereira, G. V., Parycek, P., Falco, E., & Kleinhans, R. (2018). Smart governance in the context of smart cities: A literature review. *Information Polity*, (Preprint), 1–20.

Popescul, D., & Genete, L.-D. (2016). Data security in smart cities: challenges and solutions. *Informatica Economică*, *20*(1).

Presley, S. S., & Landry, J. P. (2016). A Process Framework for Managing Cybersecurity Risks in Projects. *SAIS 2016 Proceedings*, 3–7. Retrieved from http://aisel.aisnet.org/sais2016/8

Recker, J. (2013). Scientific Research in Information Systems. In *Animal Genetics* (Vol. 39).

Reddy, D., & Rao, V. (2016). Cybersecurity Skills : The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance. *Twenty-Second Americas Conference on Information Systems, San Diego*, (2009), 1–5.

Sen, R. (2018). Challenges to cybersecurity: Current state of affairs. *Communications of the Association for Information Systems*, *43*(1), 22–44.

Sensative. (2019). Digital Malmö: A Sensative City Empowered By Yggio. Retrieved May 28, 2019, from https://sensative.com/2019/01/digital-malmo/#

Shim, J. P., Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., & French, A. (2019). The transformative effect of the internet of things on business and society. *Communications of the Association for Information Systems*, *44*(1), 129–140. https://doi.org/10.17705/1CAIS.04405

Silva, B. N., Khan, M., & Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, *38*, 697–713.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA.

Smith, C., & Miessler, D. (2014). Internet of Things Research Study. *Research Development Review*, 1–6. Retrieved from http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., … Martinez-Balleste, A. (2014). Smart health: A Context-Aware Health Paradigm within Smart Cities. *IEEE Communications Magazine*, *52*(8), 74–81. https://doi.org/10.1109/MCOM.2014.6871673

Stockholms stad. (2017). How the smart city develops. Retrieved May 28, 2019, from https://international.stockholm.se/governance/smart-and-connected-city/how-the-smart-city-develops/

Subramanian, R. (2016). *Historical Consciousness of Cybersecurity in I*ndia.

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, *40*(4), 853–865. https://doi.org/10.1109/TSMCA.2010.2048028

The Triangle Admin. (2015). Benefits of using Nvivo for data management. Retrieved from https://researcholic.wordpress.com/2015/04/20/benefits-of-using-nvivo-for-data-management/

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Vattapparamban, E., Güvenç, I., Yurekli, A. I., Akkaya, K., & Uluağaç, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. *2016 International Wireless Communications and Mobile Computing Conference, IWCMC 2016*, 216–221. https://doi.org/10.1109/IWCMC.2016.7577060

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Yang, S.-K., Kwon, Y.-J., & Lee, S.-Y. T. (2018). The Impact of Information Sharing Legislation on Cybersecurity Industry. *Thirty Ninth International Conference on Information Systems*, (July 2018), 1–16. Retrieved from https://fas.org/sgp/crs/misc/R45127.pdf

Zhang, Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. https://doi.org/10.1109/MCOM.2017.1600267CM

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments. *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, (2007), 1328–1334. https://doi.org/10.1109/CIT.2010.501

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592.