BankID-based Authentication for Phone Calls

ANTON GÖRANSSON
EMMA ASKLUND
MASTER´S THESIS
DEPARTMENT OF ELECTRICAL AND INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING | LTH | LUND UNIVERSITY

BankID-based Authentication for Phone Calls

Anton Göransson `dat14ago@student.lu.se`

Emma Asklund `dat14eas@student.lu.se`

Department of Electrical and Information Technology
Lund University

Supervisor: Martin Hell
Co-supervisor: Sandra Olsson, Telavox

Examiner: Thomas Johansson

January 20, 2020

© 2020
Printed in Sweden
Tryckeriet i E-huset, Lund

Abstract

Authentication for phone calls is important for companies with hundreds of customers wanting to access sensitive information. However, it is sub-par compared to authentication when using applications or websites.

In this thesis, seven models have been developed for how to use BankID as the authentication service during phone calls. The purpose of all models is to use the BankID API to provide the agent with the caller's personal identity number and name. Two models, "manual recitation" and "the SMS model", were selected and implemented based on criteria of security, ease-of-use, and integration to the existing environment.

In the manual recitation model the agent asks the caller to read their personal identity number aloud, the agent then starts the BankID authentication process using the personal identity number.

In the SMS model the agent sends out an SMS to the calling number, this SMS contains a link where the caller can start the BankID authentication process.

The implementation has been used in production with real customers and evaluated using questionnaires, interviews, and tracings. Our results showed that BankID can be used for authentication during phone calls, improving security while still being easy to use.

Acknowledgments

We would like to thank our supervisor at Telavox, Sandra Olsson for the help during this thesis project. You helped us to find an interesting project, came with helpful tips during the entire process, answered all our questions or guided us to someone that could, and made us feel welcome at Telavox. We would like to thank Henrik Thorvinger for help during the brainstorm process giving us innovative ideas, and for your help to find real customers of Telavox evaluating the prototype. We would also like to thank Martin Larsson at Telavox for helping us start our thesis at Telavox and for answering specific questions about the development. Sandra and Martin and many more employees at Telavox helped us with code reviews, interviews, and questions about Flow - we would like to thank you all for your time and helpful advises.

Finally, we would like to thank Martin Hell for the support during the process making sure the thesis resulted in a high quality.

Popular Science Summary

How come authentication for phone calls is so much different from when accessing a website or an application? In a world where security is becoming increasingly important, it shouldn't be. We have implemented two solutions using the electronic identification service BankID in order to improve authentication for phone calls, while still maintaining a smooth experience for the caller.

To verify that it is really your mother calling you is easy. First you recognise her phone number and when you answer, her voice. But what happens if you are an agent that gets hundreds of calls a day and from people that are strangers? A phone number can easily be faked and if the agent does not recognise the voice, how does the agent know who they are talking to? Even if they happen to recognise the voice, that is not sufficient anymore because of fraudsters using AI deepfakes to mimic voices.

Currently, many companies only check that the phone number exists in their customer system. However, the phone number can easily be faked, allowing fraudsters to access sensitive information or make orders in a company's name. To avoid this, we have implemented two solutions using the Swedish electronic identification service BankID in order to authenticate the caller. BankID is used in many services, mainly on the web and in mobile applications and is becoming increasingly popular with over 80% of the Swedish population using it. By integrating BankID, it allows the agent to verify the caller's personal identity number and name from BankID. After verifying that the personal identity number exists in the customer system, the authentication is complete.

Our first solution requires the caller to read their personal identity number aloud while the agent enters it in a webpage starting the BankID authentication process. When the caller has completed the process, the agent will receive the caller's personal identity number and name. Some other companies use this solution as well, but this solution has some drawbacks. First, the caller must share sensitive information via the phone and with privacy becoming more important they might be more reluctant to do so. Second, the agent can hear or enter the personal identity number incorrectly, reducing the quality of the call.

In our second solution, the agent instead sends an SMS to the calling number with a link. This link comes with a unique token and is only valid for 10 minutes. When the caller follows the link, they will come to a webpage where they can open BankID instantly on their current device or enter their personal identity number and open BankID on another device. This solution removes the risks of human errors and puts the caller in control of what they are sharing with the same result for the agent.

Both these solutions verify who the agent is talking to, similarly to when someone shows their physical identification, e.g. a passport. But our solutions only involve collecting the caller's information, the agent is still required to verify that information in their customer system. I.e. to verify if the caller has access to the services he/she asks for, e.g. changing a password. Meaning that our solutions rely heavily on the persons using them to guarantee the correctness.

In our work we have evaluated our solutions through interviews and in production use. The results showed that the security during the call would increase without being too cumbersome to use. This means that companies can feel more secure about who they give sensitive information to.

Table of Contents

1 Introduction **1**
- 1.1 Problem Definition . . . 1
- 1.2 Limitations . . . 2
- 1.3 Related Work . . . 2
- 1.4 Literature Study . . . 3

2 Background **5**
- 2.1 Social Engineering . . . 5
- 2.2 Electronic Identification . . . 6
- 2.3 BankID . . . 7
- 2.4 Telavox . . . 12

3 Method **17**
- 3.1 Procedure . . . 17
- 3.2 Selecting Electronic Identification . . . 17
- 3.3 Finding and Creating Models . . . 18
- 3.4 Implementation of Models . . . 18
- 3.5 Empirical Study . . . 18

4 Selection of Models **21**
- 4.1 Initiating a BankID Authentication Request - Block A . . . 21
- 4.2 Showing Authentication Result - Block B . . . 24
- 4.3 Storyboards . . . 25
- 4.4 Interesting Models . . . 30
- 4.5 Selection of First Implementation . . . 33
- 4.6 Selection of Second Implementation . . . 33

5 Implementation **35**
- 5.1 The Manual Recitation Model . . . 35
- 5.2 The SMS Model . . . 36

6 Evaluation **41**
- 6.1 Questionnaires . . . 41
- 6.2 Interviews . . . 42

6.3 Target Group 44

7 Result **45**
7.1 Questionnaire 45
7.2 Tracings on Prototype 45
7.3 Interviews 46

8 Discussion **51**
8.1 Key Management 51
8.2 GDPR 51
8.3 Implementation 52
8.4 Tracings 52
8.5 Interviews 53
8.6 Questionnaires 54
8.7 Effects on Product 55
8.8 Improvements 56
8.9 Future Work 56

9 Conclusions **57**

References **59**

A BankID Web Service API Request and Response Examples **63**

B Questionnaires for Agents and Callers **67**
B.1 Caller's Questionnaire 67
B.2 Agent's Questionnaire 67

C Interview Questions **71**
C.1 Interview Questions 71

D Results from the Questionnaires **73**
D.1 Agent Questionnaire 73
D.2 Caller Questionnaire 75

List of Figures

2.1 A flowchart of the events when a user accesses a RP's service integrated with BankID. 10
2.2 A screenshot of the Flow Admin application, showcasing a private branch exchange service. 13
2.3 A screenshot of the application when someone is calling you. 14
2.4 A screenshot of the web application and how the telephone switchboard looks. 15
2.5 A screenshot of the Telavox website with the Flow Widget open in the bottom right corner. 15

4.1 A flowchart of Block A. Showing how a BankID authentication request can be initiated before or during a phone call. 23
4.2 A flowchart of Block B. Depicting the different solutions to handle the response from the BankID web service API. 27
4.3 A storyboard for manual recitation with both the caller's and the agent's view. 28
4.4 A storyboard for DTMF with two different ways to come to the solution that the caller enters their PN in the keypad on the phone. 29
4.5 A storyboard for SMS with two different ways to come to the solution that the caller receives a link via SMS where they can initiate a BankID authentication request. 30
4.6 A storyboard for collecting the PN from a database based on the callers phone number with both the caller's and the agent's view. . . 31

5.1 The agent's view before initiating the authentication process. 37
5.2 The agent's view when the authentication process is running. 37
5.3 The agent's view when the authentication was successful. 38
5.4 The agent's view when an authentication process is already running for the phone number entered. 38
5.5 The caller's first view after pressing the link in the SMS the agent sent. 38
5.6 The caller's view when they should open their BankID app. 39
5.7 The caller's view when their token is already used or old. 39
5.8 The caller's view when something went wrong. 39

5.9 The caller's view when the authentication was successful and they can go back to the call. 39

6.1 Where the agents can find the questionnaire 43
6.2 Where the caller can find the questionnaire 43
6.3 Picture of the SMS we sent out after the call. 43

A.1 Example authentication request to the BankID server. 63
A.2 Example answer from the BankID server when sending an authentication request. 63
A.3 Example request sent from the relying party to the BankID server to get status about a authentication request. 64
A.4 Example response from the BankID server when the status of the authentication is pending. 64
A.5 Example response from the BankID server when the status of the authentication is complete. 65

D.1 Responses on question one from the agent's questionnaire. 73
D.2 Responses on question two from the agent's questionnaire. 73
D.3 Responses on question three from the agent's questionnaire. 74
D.4 Responses on question four from the agent's questionnaire. 74
D.5 Responses on question five from the agent's questionnaire. 74
D.6 Responses on question one from the caller's questionnaire. 75
D.7 Responses on question two from the caller's questionnaire. 75
D.8 Responses on question three from the caller's questionnaire. 75
D.9 Responses on question four from the caller's questionnaire. 76
D.10 Responses on question five from the caller's questionnaire. 76

List of Tables

4.1 A summary of the security flaws for each authentication model using BankID. 25
4.2 A summary of the usability pros and cons for each authentication model using BankID. 26

6.1 The research question which each interview question is related to. The interview questions can be found in Appendix C 44

7.1 Short answers from the interview, the questions were asked after each case. 47
7.2 Short answers from the interviews asked after the three cases. 48

Glossary and Abbreviations

In this paper we will use some words and abbreviations that you may not have heard before, here is an explanation of those words and abbreviations.

- **Agent**
  Person working for an organization, receiving phone calls from customers. For example, someone working in a help desk.
- **API** - Application Programming Interface
  We will specifically be using a web API which is an interface consisting of publicly exposed endpoints to a defined request–response message system.
- **CRM** - Customer Relationship Management
  The system a business uses to handle their customers.
- **DTMF** - Dual Tone Multi Frequency
  When you press a button on a phone or a phone's keypad a signal with two frequencies is produced. This tone can be used to identify which button was pressed.
- **Flow**
  The main product sold by Telavox where we integrated our prototype.
- **KBA** - Knowledge Based Authentication
- **OTP** - One Time Password
- **RP** - Relying Party
  The RP uses the BankID web service authentication and/or signing functionalities to for example provide login functionality to the end-user.
- **PN** - Personal Identity Number
  PN is a unique number for every person living in Sweden. It is often used to identify individuals at different authorities in Sweden.
- **SIM Swap Attack**
  A fraudster transfers a victim's phone number to their own SIM card and gains full access to the victim's phone number.
- **Spoofing**
  Spoofing is when using a fake or stolen identity.

- **TLS** - Transport Layer Security
  A cryptographic protocol used for secure communication over a computer network.

Chapter 1

Introduction

Verifying someone's identity when they call you is usually recognition based. For example, if your friend calls you, you almost at once recognize the number, identify their voice or identify their way of talking. If you want to call someone you look up their number and when you call it you know who you will be talking to. But if you run a large company with hundreds of customers asking to order products, reset passwords, access sensitive data, etc, it is impossible to recognize everyone calling in. It is also easy to spoof the number you are calling from making it more difficult to trust. Some companies use security questions or try to ask for information that only the person who the caller claims to be should know. If you compare these methods to when you show a physical identification from the government or when you sign into a web page using two-factor authentication, the verification during phone calls is very weak.

It is of course possible to have the caller go to a web page and sign into the company's service or have the caller find their physical identification, take a picture of it and send it in. But these methods easily become cumbersome and will take away from the experience of the caller.

We will provide a solution using the Swedish electronic identification service; BankID. We describe how BankID works and why it fits in our solution. This solution will allow the company to verify the caller in a legitimate way and it will be as simple to use as possible.

1.1 Problem Definition

BankID is widely integrated in many different services, but there are barely any integrations for phone calls. Our thesis will answer the following research questions to better understand how it affects phone calls and if we can make phone calls more secure using BankID as the method of authentication.

Q1: Which models can be used to integrate BankID during a phone call?

Q2: Which of these models fits the following criteria the best?

  a. Ease of use.

  b. Risk of stolen identity (e.g. social engineering).

Q3: How does an implementation affect the current product according to the criteria?

  a. Ease of use.
  b. Risk of stolen identity.

1.2 Limitations

Our solution will only be working in Sweden since we will use the Swedish service BankID. Other types of electronic identification might lead to a different implementation. When creating the different models, we are assuming that the caller has BankID and access to the internet. We assume that when checking with the business CRM system, the information is correct, and we will not focus on how the telephone number and/or the personal identity number entered the CRM system.

1.3 Related Work

In this section, we will mention earlier work that is related to what this thesis will be about.

1.3.1 E-legitimation Fraud: The Balance Between Trust and Deception

Sebastian Agnvall and Georg Lavman have done a thesis about frauds on electronic identification (eID) and the balance between trust and misdirection [1]. In their thesis they are answering the question; Which challenges are eID, for example, BankID, facing when trying to neutralize threats where the threat exploits the human factor? They mention different attacks known for targeting BankID and have interviewed different people working with IT security and investigating IT frauds to understand the problem better.

The reason they have chosen to answer their question is that there are now over 7 million people in Sweden using BankID and the weakest link in the system is the person using it. The criminals wanting to use the weak spot of BankID is looking into the human being and sees that they can use the human's trust to manipulate and misdirect them to get them to sign with BankID on malicious requests.

In the end, the writers concluded that increasing the awareness of the weakness of the application was the best way to make it secure. Below are the three technical ways they suggested increase awareness:

- Use direct communication to the user using only the primary communication interface.
- Use two-sided authentication; the user authenticates the bank and the bank authenticates the user.
- Provide a course that every user must pass to get access to use BankID.

This relates to our work because the security we chose to add to the phone call is eID and Agnvall's and Lavman's paper is about how to make and use the eID as safe as possible. They use BankID as their main eID - the same as we do and because we add security to a phone call which is highly exposed to social engineering attacks, this report relates to our work because it talks about how secure BankID is against social engineering attacks.

1.4 Literature Study

In this section will we mention studies that are important for our research. We will make references to these papers when analysing and making decisions about our models and implementation.

1.4.1 Caller Authentication

According to Terry L Nelms there exist four ways to authenticate a caller [21]. Knowledge-based authentication (KBA), SMS one-time password (OTP), caller ID matches phone number on file, and voice bio-metric.

KBA is when the caller answers questions about themselves which only they should know, this needs added enrolment and the attackers can find the answers online because of social media. When the agents collect the answers, the caller might feel interrogated which lessens the experience of the call and might make the caller hesitant to call again. KBA does not need any devices or technology which Nelms considers a good aspect.

OTP is when the agent sends a one-time password by SMS to the phone number in file to authenticate the callers. This method uses SMS, which is very widespread, and the caller enrolled their phone number in the system, so the caller does not need to add more information to their enrolment later. Cons with this method are that it is very exposed to social engineering and the agent puts a lot of trust in the phone number on file. Another con is that this method exposes the agent to the SIM swap attack, a phone number is not a physical thing, it is virtual, and this attack has become more heavily used during the last years.

Companies matches caller ID with number on file to see if the caller's ID is matching what they can see in their system. This is a seamless authentication and the caller has already enrolled their phone number so in the authentication process, the caller does not need to do anything for the agent in order to be authenticated. Cons with this method is that it is vulnerable to spoofing and SIM swap attacks. With this method, the enterprise needs to trust that the phone number in the file is correct.

If a company uses voice biometrics to authenticate a caller, the voice biometric extract some features from the caller's speech and compared to a voice print collected earlier from the user that the caller claims to be. One pro with this method is that it authenticates the actual caller, and not who it is supposed to be, without the caller needing to do anything. A con is that the voice can change, for example, if you have a cold or when you are getting older. To be able to have anything to compare the caller voice to you need to have enrolled a voiceprint earlier and you have to talk enough during the call to be able to compare the speech to the voiceprint during the call and that can take some time.

Nelms concludes that building trust for security authentication during a phone call is challenging and costly. And to have any use of authentication the trust needs to be mutual, the caller need to trust that they have called the right person and the callee needs to trust that the caller is who he or she claims to be.

1.4.2 Trust the Caller

It is easy to send an SMS and to make a call impersonating another person or a company [7]. Many companies warn their customers not to trust emails and only to trust phone calls or SMS but since caller ID spoofing has become more available for forgers this is not safe either. You could trust a phone call when all the phones were plugged into the wall because then, all the phones could be traced to a location and all phone activities had to be able to be sent if asked, according to the law. With mobile networks you do not get the information by looking at the number, you can buy a SIM card without showing identification and the location of a mobile phone changes and therefore spoofing attack are easier to carry out.

Chapter 2

Background

In this chapter, we describe the theoretical background related to this thesis. We will be describing social engineering which is the most common type of attack via phone calls, electronic identification, and public key infrastructure. We have chosen to use BankID as our authentication method, and we will describe the service along with common methods that fraudsters use to exploit BankID.

All this information we will later take into consideration when choosing a model and analysing the implemented models.

2.1 Social Engineering

Fraudsters have designed social engineering techniques specifically to target IT security countermeasures [20]. Ian Mann explains social engineering as attacking what is missing between physical security and IT security [20] and define it as, “To manipulate people, by deception, into giving out information, or performing an action” [19]. Mann’s definition is similar to Kaushalya, Randeniya, and Liyanage’s, “The art of exploiting human behavioural and emotional loopholes in order to gain access to secure data is social engineering” [14].

It is easier to make a web server technically secure than making it secure against social engineering, since even if a web server can be complex, a human is even more complex. A human has been “programmed” their whole life and there are millions of us so we can be infinitely complex. Hackers use the human’s weaknesses to find the best way to hack a system. Social engineering gives the hackers the protection of anonymity and distance [19], but not everyone can pull this type of attack off [14]. The attacker must be skilled in human manipulation and feed a person false information to fool the judgment of the person they are attacking.

By not treating social engineering as a serious attack, people make themselves more prone to the attack. For this reason, the people that do not expect to be a victim becomes a victim without realising it. The information asked for during an attack may seem to be safe to share with a stranger but is in fact, the reason the attack works [14].

2.2 Electronic Identification

Electronic identification (eID) is an electronic identification document used to legitimize oneself securely on websites and e-services. Sweden currently has four different eID providers; BankID (provided by Finansiell ID-Teknik BID AB), AB Svenska Pass, Telia E-legitimation and Freja eID+. There are two types of eID; soft and hard. Soft eID comes with a file that is downloadable to the user's device and hard eID comes on a chip on a plastic card [11].

The eID can be used to create electronic signatures which are considered more secure than handwritten signatures since electronic signatures also hold information about if the document has been tampered with since signing. The cornerstones of electric signatures are identification, signing and encryption. These services are all provided by a public key infrastructure (PKI).

It is important to distinguish digital signatures and electronic signatures. Andreas Halvarsson and Tommy Morin define digital signatures as a technology that is used in many different areas, everything from electronic signatures to network security [13]. Electronic signatures are the solution that can be a digital replacement for a legally binding signature. Thus, digital signatures describe a technology and electronic signatures has a wider definition with a focus on the legal aspect.

2.2.1 Public Key Infrastructure

All types of electronic identification use a PKI. A PKI is a foundation for security services, it does not provide any business functionality by itself. The main purpose of a PKI is to enable distribution and use of public keys and certificates with security and integrity [13].

A PKI can implement the following security services which are important for electronic identification [29]:

- **Confidentiality** - Ensures that the secrecy and privacy of data such as personal information is provided with cryptographic encryption mechanisms.
- **Integrity** - Ensures that the data such as emails or messages are not tampered or interfered with.
- **Authentication** - Ensures that the identity of the entities can be verified.
- **Non-repudiation** - Ensures that someone can not deny the validity of something such as a message or a transaction.

A PKI also supports issuing, verifying, and revoking of certificates. A certificate is a proof of the connection between a pair of public and private keys and a person, company, or computer system.

When handling keys, key management becomes a must. Key management includes the generation, exchange, storage, usage, crypto-shredding (destruction) and replacement of keys and it is a known challenge for large organisations [10].

2.2.2 General Data Protection Regulation

When identifying an individual some amount of personal information is usually needed to be able to confirm that someone is who they claim to be and when handling any personal information, the General Data Protection Regulation (GDPR) needs to be considered. GDPR is a law put in force 25 May 2018. It regulates the handling of personal data for all citizens of the European Union (EU) and the European Economic Area (EEA) [12]. Personal data is defined as “Information that can directly or indirectly identify an individual” and it includes data such as IP address, cookie information and digital fingerprint, making the concept very wide. Data protection is the core of GDPR, and it is reinforced through transparency and accountability. Transparency includes presenting the full information to the individual about how the data is going to be handled and accountability includes that the organization responsibly handles the data. Accountability also requires organizations to implement the technical and organizational functions to be able to demonstrate how the data was handled, which might require a large restructure of their system. One of the key changes to processing personal data is consent, it is now needed anytime personal data is collected. The information when collecting personal data needs to be informative, clear and specific.

The personal identity number (PN) in Sweden is used to uniquely identify a person and is considered to be extra valuable personal information [9]. It should, therefore, be exposed as seldom as possible. The GDPR law requires that the handling of PNs should be restrictive and that there needs to be a consideration of the need for the handling of data and the risks to the integrity that comes with it.

2.3 BankID

BankID, is as mentioned in Section 2.2, one of the top four providers of eID in Sweden. Finansiell ID-Teknik, which is the company that owns BankID, estimates that 8 million of the approx. 10 million population will be using BankID at the end of 2019 [17, 25]. This means that 80% of the population will be using BankID and in the age group 21-50 Finansiell ID-Teknik estimates that 97.5% of the population already is using BankID. Thus, it is widely adopted, and a majority of the Swedes are familiar with the service.

There are 10 banks providing the BankID service for individuals, they are; Danske Bank, ICA Banken, Handelsbanken, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Swedbank och Ålandsbanken. There are three ways to use BankID; mobile, card and file. Mobile has gained a lot of traction and Finansiell ID-Teknik estimates that 7.5 out of the 8 million that will be using BankID at the end of 2019 will be using mobile. It is by far the most used of the three types with 96.7% of all usages (signings and identifications) being done via mobile. Finansiell ID-Teknik estimates a total of 4 billion usages of BankID in 2019, which is almost a billion more than the year before [18].

To be able to integrate BankID into a service, the organisation who wants to provide the service (the relying party) first needs to contact one of the banks that sell the certificate to get access to BankID’s API, these banks are Danske Bank, Handelsbanken, Nordea, SEB and Swedbank. There is usually a starting price and then a cost for each signing and identification. The organisation gets access to all BankID users, regardless of bank.

2.3.1 How it Works

Users must install the BankID app on their mobile device or PC to be able to use the identification and signature features. They also need to order a BankID from their bank. The relying party (RP) uses the BankID web service, which requires a valid TLS client certificate, otherwise, they cannot reach the web service API.

If the RP's service executes on the same device that has the BankID app installed, it is possible to automatically launch the app via the RP service and the user does not need to enter their PN. Otherwise, if the RP's service is running in a web browser on a different device, the user must manually start the BankID app and enter their PN in the RP's service [6]. When the end-user receives the authentication request a screen appears, displaying the organization that the user is verifying to. There is also an input, where the end-user enters their PIN number to verify who they are. It is also possible to use fingerprints for some services instead of a PIN.

2.3.2 QR-Code

A Quick Response (QR) code is a two-dimensional symbol invented in 1994 and ISO approved it an ISO standard 2000. QR codes can hold large amounts of data and has high performance. A common use-case, especially in marketing is to let the QR code link to a website, removing the need for the user to open their web browser manually and typing in the URL [27].

BankID implemented QR codes in September 2018 to strengthen the secure use of BankID [5]. By forcing the user to have to read the QR-code it ensures their physical presence during the authentication.

2.3.3 Test Environment

BankID provides a test environment for a RP. It consists of an TLS client certificate given by BankID to communicate with their test web service API. This requires configuration of key stores and trust stores where the RP handles public/private key pairs and certificates. There is also a special BankID test app that needs to be set up on mobile or PC [6]. This test environment makes it possible to set up a working integration with BankID without being in contact with a bank, saving both time and money.

2.3.4 Web Service API

The two main endpoints of the BankID web service API that we intend to use are `/rp/v5/auth/`, which is used for verifying a user's identity, and `/rp/v5/collect`, which is used for collecting the result of an authentication or a sign request. From now on an auth request refers to when the RP sends a request to the `/rp/v5/auth/` endpoint and a collect request refers to when the RP sends a request to the `/rp/v5/collect` endpoint. There are examples of requests and responses that we will be using in Appendix A.

When the RP sends an auth request with or without the PN the BankID web service API will respond with an `orderRef` which refers to that authentication and an `autoStartToken`. The RP then uses the `orderRef` for the collect request, to receive information about that authentication. The RP uses the `autoStartToken` to automatically open the BankID app on the user's device.

2.3.5 Basic Use Cases

BankID describes the most common basic use cases in their RP guidelines [6]. The most common cases of accessing the RP's service include the following; using a browser on a PC, using a browser on a mobile device, and using a native application on a mobile device. We describe the use case most relevant for us, accessing the RP's service using a browser on a mobile device, below.

- Users should be asked if they want to login or sign using "Mobile BankID on this device" or "Mobile BankID on another device".
    a. Users that select this device does not need to enter their PN and the RP must start the BankID app on the mobile device
    b. Users that select to use another device and the RP does not support QR code needs to enter their PN and manually open the BankID app on another device.
    c. Users that select another device and the RP supports QR code needs to manually open their BankID app on the other device and scan the QR code.

2.3.6 Flow of Events

BankID also describes the flow of events when a user interacts with the service of the RP which is using BankID [6]. They are as follows:

1. The RP ask the users that select "another device" to enter their PN if the RP does not already know it or has it saved. QR codes may be used as an alternative to entering the PN.
2. The RP uses the auth or the sign method of the BankID web service API to initiate the order. The web service returns an `autoStartToken` and an `orderRef`.
3. If the user selected "same device" the RP tries to start the BankID app. The RP uses the `autoStartToken` in the start command if the user is not providing their PN in the web service call. Once the BankID app has finished running it will return to the previous process.
4. If the RP supports QR code, the RP creates a QR code based on the `autoStartToken`, which the user scans.
5. The RP's service displays a progress indicator.
6. The auth or the sign order is displayed in the BankID app and the RP's name as they stated it in the RP certificate, is displayed. The user enters their personal security code, verifies with fingerprint, or cancels the order.

7. The RP periodically uses the collect method of the web service API until they receive a final response. At the same time, the RP is continuously updating the user's information message.
8. The RP removes the progress indicator.

In Figure 2.1 this flow of events and how the RP is communicating with the BankID web service API can be seen.

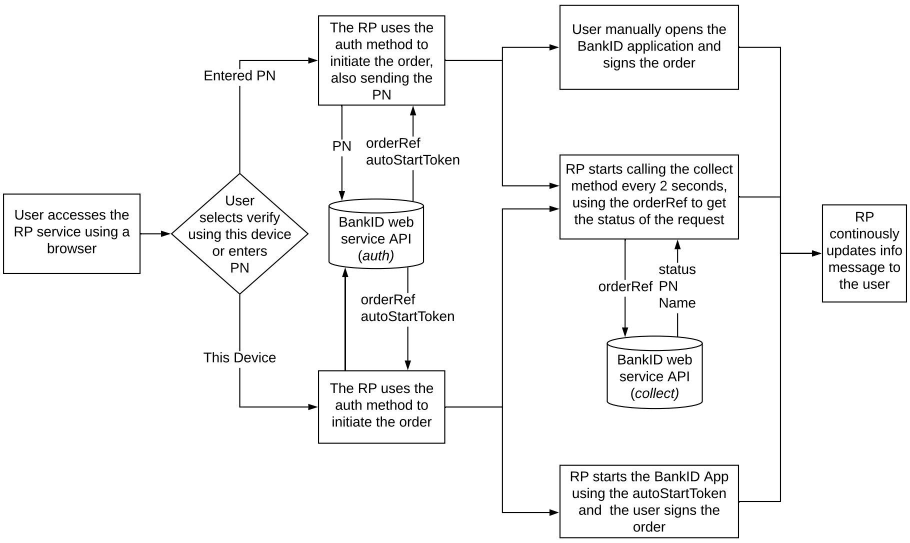

User accesses the RP service using a browser
User selects verify using this device or enters PN
Entered PN
This Device
The RP uses the auth method to initiate the order, also sending the PN
PN
orderRef
autoStartToken
BankID web service API (*auth*)
orderRef
autoStartToken
The RP uses the auth method to initiate the order
User manually opens the BankID application and signs the order
RP starts calling the collect method every 2 seconds, using the orderRef to get the status of the request
orderRef
status
PN
Name
BankID web service API (*collect*)
RP starts the BankID App using the autoStartToken and the user signs the order
RP continously updates info message to the user

Figure 2.1: A flowchart of the events when a user accesses a RP's service integrated with BankID.

2.3.7 Existing Implementations of BankID for Phone Calls

Soluno who is offering a corporate telephony solution has integrated BankID into their product. In their implementation, the agent asks the caller to read their PN aloud. The agent enters the PN into the user interface on the website that Soluno provides. The caller then opens their BankID app and signs the request, if the authentication was successful the agent will see that verification was successful [26]. Soluno provides the BankID certificate for the customer.

Easy Teams is another company that provides a corporate telephony solution with BankID integrated. Their solution is similar to Soluno's, with a website where the agent enters the phone number and the caller having to open BankID manually to sign [28].

Netnordic offers system integrations with a focus on network, data centres, security, and telephony. Their implementation is automatic and when a customer calls the call centre, a voice asks them about their PN that Netnordic will use for verification. The caller then enters their PN using the keypad and starts their

BankID app. If the verification is successful, the caller is sent to a group where an administrator takes the call. If the verification fails it is possible to send the call to an administrator with the information that it failed to be able to verify it manually instead. They do not provide any certificates; you have to contact the banks yourself to use the BankID integration [22].

ICA Banken is one of the banks providing BankID. When calling their support an automated voice tells the caller that before talking to one of their agents, they need to verify themselves. ICA Banken has chosen to do the verification using DTMF where an automated voice tells the caller to enter their PN in the keypad and finish with #. Then the automated voice tells the caller to open their BankID application and finish the authentication. When the caller has completed these steps, the caller goes to a queue where they will get to talk to an agent eventually. When it is their turn the agent can directly see the caller's information without the caller telling the agent who they are.

All these methods of verifying are analysed further in Section 4.1.

2.3.8 Certificate Handling

There are three methods to handle the RP's certificates. First one is that the RP (in our case Telavox) has their own certificate and their server handles all authentication and verification requests. Second is that the organization that is buying the product provides their own certificate and they handle their own requests. And the third one is that Telavox handles the certificates, but it will be one certificate per organisation that buys the product.

The advantages of having Telavox handle the requests (first method) are that there will then only be one RP, which means only Telavox needs to buy a certificate. Since Telavox and their customers will make a lot of requests, Telavox can make an advantageous deal with the bank for the pricing as well. One problem is that when signing via the BankID app, Telavox will always be the organization name shown in the prompt, the customers of the buyer might never have heard of Telavox before and therefore be suspicious of signing. Another problem is that Telavox does not have any control of how many callers that their customers will verify, meaning some customers might abuse it resulting in large costs for Telavox.

Letting the organizations acquire their own certificate (second method) makes the threshold of starting larger but it can also be a service that Telavox provides similar to Soluno, where they help you acquire a certificate for a cost. Letting organizations have their own certificate allows more transparency for their customers and they can manage the fee to BankID on their own, adjusting it according to the number of requests. The product will also be more contained if the buying organization handles the certificate resulting in fewer ways to attack the system.

To let Telavox handle the certificate but have different ones for each company using the (third method) has the pros of the first one with making it easy for organisations to buy and start using Flow. And with this method, the BankID prompt will show both Telavox name and the organisation that bought Flow and the customers of the buyer can recognize the correct name.

2.3.9 Common Frauds

In Agnvall and Lavman's thesis described in Section 1.3.1, they were asking if attacks against BankID could count as social engineering and all the individuals interviewed answered yes. Jan Olsson answered of course because they are using the phone to fool people and Albin Zuccato agreed, saying that it is not an attack on the technique or algorithm, they attacked the weakest link which in this case is the human. Boris Berberovic said that it was a case of social engineering, but he also counts it as a bug, like a weak spot in the system. The BankID system is secure and impossible to hack so the fraudsters must go via the weakest link; the human.

During one type of attack the fraudsters randomly call phone numbers that they can connect to a PN and they say that they are from the bank's security department, the police, or another authority. They then explain that there is unusual activity on their account and that the victim needs to sign using their eID. Simultaneously the fraudster prepares a sign-in to the victim's internet bank and when the victim signs the fraudster receives access. Now the fraudster can transfer money from the victim's account, they need to convince the victim to sign one more time though, to approve the transaction. The fraudster then launders the transferred money, and it is impossible to get it back [4].

In September 2018 BankID started to support QR codes, this was to reduce frauds since the individual logging in via BankID needs to have access to the physical phone [3]. Combined with people obtaining more knowledge of how the fraudsters are operating, the voice phishing attacks reduced by 90% [15].

2.4 Telavox

In this section, we will talk about Telavox and discuss their main product Flow, with a focus on the parts relevant to our work. The information found in this thesis is not only relevant to Telavox, but you can use it in other companies. But to make it easier to understand how we did our implementation this section will provide some information about Telavox and Flow.

2.4.1 About Telavox

Telavox is a global IT-company that two students from Lund founded in 2003. The main product they sell is Flow, a system that has everything needed to communicate and collaborate in a company, which today has more than 250 000 users. The company is cloud based and has been since the start.

Flow consists of three parts; Flow Admin, the web application and the Android and iOS applications (which have the same functionality as the web application). Flow Admin is where the administrator can do all the administration, here the administrators at a company can control everyone's permissions, create users etc. Administrators and managers use Flow Admin while Flow App, which exists as both a web application and a phone application, is what most employees use. This application is a place to chat, make group chats, have video chats and to answer phone calls. It is also where the employees that work with customer services work and can see the telephone switchboard and answer calls. We will go more in-depth about what Flow does in the sections below.

2.4.2 Flow Admin

The Flow Admin application's main user base is the administrators of the company that uses Flow. It is possible to administrate almost everything related to users and telephony. The main functionality is to be able to bulk handle user settings, it is also possible to design private branch exchange (PBX) services. In Figure 2.2 the user interface for designing a PBX service is shown. Calling in to a designated number will put the caller in the "Demo Queue", then depending on the schedule, the caller will be connected to an agent, played a sound clip before it hangs up or continuing to a button selection.

This user interface allows administrator to design complicated PBX services with ease and this is the main way to work with a PBX. It is also possible to interact between the different steps of the service through scripts.

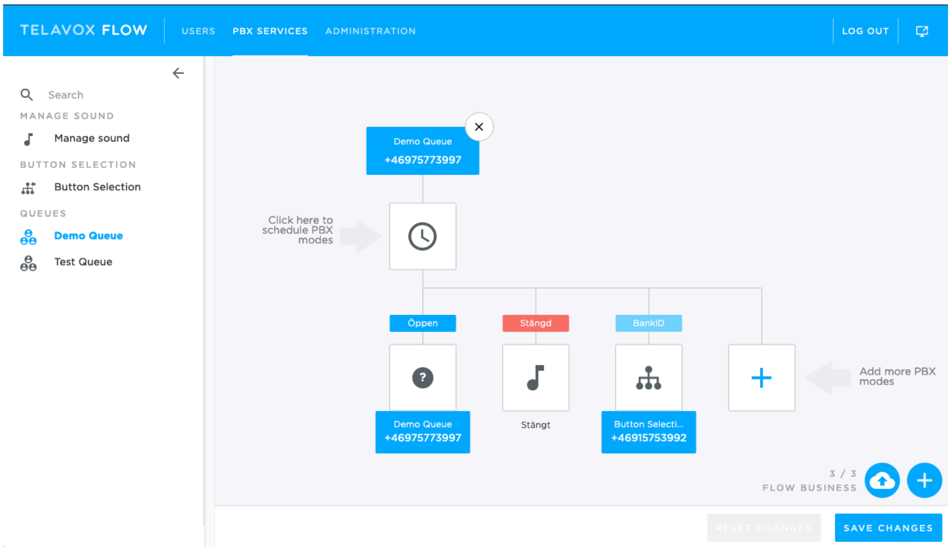

TELAVOX FLOW
USERS
PBX SERVICES
ADMINISTRATION
LOG OUT
Search
MANAGE SOUND
Manage sound
BUTTON SELECTION
Button Selection
QUEUES
Demo Queue
Test Queue
Demo Queue
+46975773997
Click here to schedule PBX modes
Öppen
Stängd
BankID
Demo Queue
+46975773997
Stängt
Button Selecti...
+46915753992
Add more PBX modes
3 / 3
FLOW BUSINESS
RESET CHANGES
SAVE CHANGES

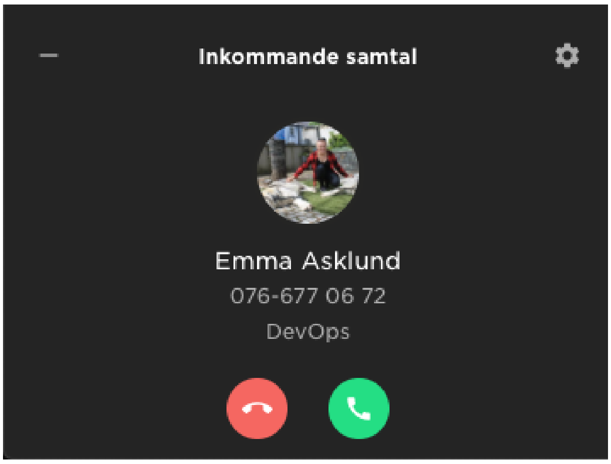
Figure 2.2: A screenshot of the Flow Admin application, showcasing a private branch exchange service.

2.4.3 Flow App

Flow App is the main application that exists both as a web application and a mobile device application. This application is where the users would spend most of their time communicating. There are four main functions; chat, phone calls, video calls and telephone exchange.

Call

A caller can call in two ways, either you call your colleague with a physical phone or you can call through the application. It is the same when it comes to answering the phone, either answer through the application or the physical phone. When someone is calling you, you receive a pop up in the corner of your screen where you get the options to answer or decline the call shown in Figure 2.3.



Emma Asklund

076-677 06 72

DevOps

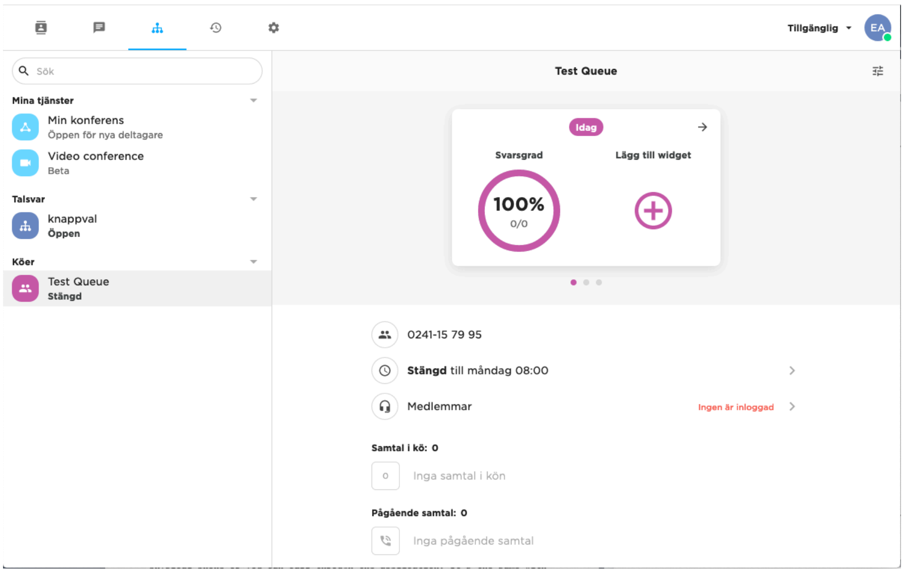
Figure 2.3: A screenshot of the application when someone is calling you.

Telephone Exchange

If you work with customer support, you need to see the telephone exchange and answer calls according to a queue. Flow has a view in Flow App for this that you can see in Figure 2.4. In this view the agents can for each queue see how many that are in the queue, how many that are in a call, and the latest call together with who answered that call.

2.4.4 Flow Widget

The Flow Widget is a small window that customers of Telavox can integrate into their website. In Figure 2.5 it can be seen integrated into Telavox's website. If a caller is browsing the website by mobile, pressing the number will open the caller's phone application with the number filled in.


Tillgänglig
EA
Sök
Mina tjänster
Min konferens
Öppen för nya deltagare
Video conference
Beta
Talsvar
knappval
Öppen
Köer
Test Queue
Stängd
Test Queue
Idag
Svarsgrad
100%
0/0
Lägg till widget

0241-15 79 95

Stängd till måndag 08:00

Medlemmar Ingen är inloggad

Samtal i kö: 0

0 Inga samtal i kön

Pågående samtal: 0

Inga pågående samtal

Figure 2.4: A screenshot of the web application and how the telephone switchboard looks.

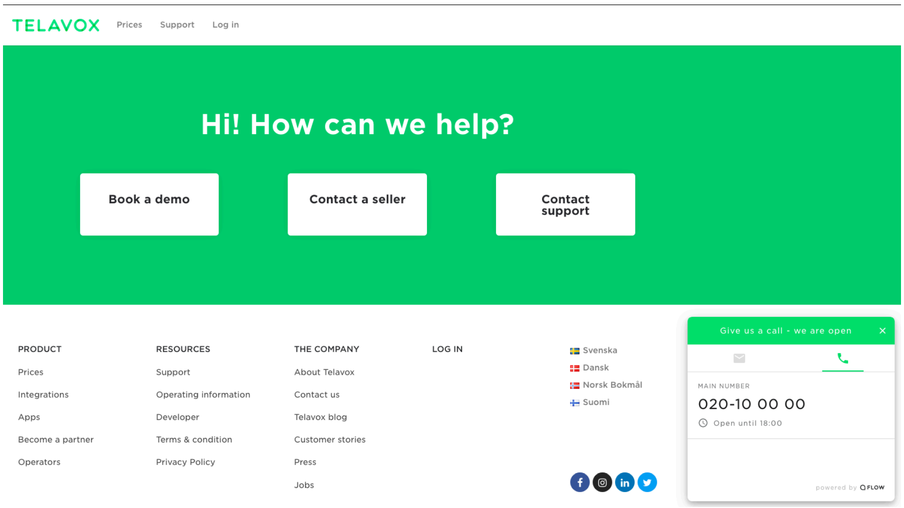

TELAVOX
Prices
Support
Log in
Hi! How can we help?
Book a demo
Contact a seller
Contact support
PRODUCT
Prices
Integrations
Apps
Become a partner
Operators
RESOURCES
Support
Operating information
Developer
Terms & condition
Privacy Policy
THE COMPANY
About Telavox
Contact us
Telavox blog
Customer stories
Press
Jobs
LOG IN
Svenska
Dansk
Norsk Bokmål
Suomi
Give us a call - we are open
MAIN NUMBER
020-10 00 00
Open until 18:00
powered by FLOW

Figure 2.5: A screenshot of the Telavox website with the Flow Widget open in the bottom right corner.

Chapter 3

Method

In this chapter we describe which steps we took during this thesis. We motivate our choice of electronic identification and describe how we found and selected models. We also describe how we made our implementations and, finally, how we performed the empirical study.

3.1 Procedure

During this thesis we took the following steps:

1. Find models for using BankID as an authentication method during phone calls.
2. Make a storyboard for each model.
3. Implement a prototype of the manual recitation model.
4. Implement a prototype of the SMS model.
5. Make questionnaires.
6. Give the prototype to the agents.
7. Perform interviews.

3.2 Selecting Electronic Identification

We decided to use BankID as the eID for our implementation since it is the most widely used eID in Sweden and it exists on both mobile and PC. As mentioned in Section 2.3 it is expected that approx. 80% of the Swedish population will be using BankID at the end of 2019. This existing user base is important because when users encounter a system which they have had no prior interaction with, they will look at “good reasons” to trust it [16]. By using a well-known eID, users will have a large amount of initial trust allowing us to focus on the implementation and not how to build up the initial trust.

BankID also has great documentation, making both the testing and production phase of our implementation as simple as possible. They also provide a test environment, which allowed us to get everything working before we made any decision about moving to production.

3.3 Finding and Creating Models

To find the different models we decided to use flowcharts. The definition of a flowchart is a formalised graphic representation of a program logic sequence, work or manufacturing process, organisation chart, or similar formalised structure [2]. Flowcharts uses symbols to represent operations, data, flow direction and equipment for a definition, analysis, or solution to the problem. We decided to use flowcharts since they are easy to use and we also estimated that the charts would not get too large and obscure, which might be a weakness of flowcharts.

When looking into the problem with authentication during a phone call we have split the problem into two different blocks. Block A is about how we can initiate a BankID auth request, where some of the solutions involve collecting the caller's PN. While Block B is about how to show the result from the BankID response to the person answering the call, usually a person in the telephone exchange and we refer to this person as agent.

3.4 Implementation of Models

We implemented the models in close collaboration with Telavox since we decided to integrate our models in Flow. We made that decision since Telavox already had all the resources for us to run our prototype live. During the implementation we looked at similar web pages Telavox had, to see how we could design and develop our implementation. Since Flow is mainly written in Java for the backend and Angular (Javascript) for the frontend those were our choices as well. We also studied the BankID documentation to be able to understand how we should communicate with the BankID web service API. When we had a working prototype our code went through several iterations of code review to make sure that it lived up to Telavox's standards.

3.5 Empirical Study

The two main ways to collect information directly from people or a specific group of people are; interviews and questionnaires [30]. Using questionnaires puts more pressure on us to have a good knowledge of the product to be able to ask the right questions, compared to an interview where the questions can change along the way. But even if the questions must be more thought through beforehand, we chose to send questionnaires to the agents and the callers for two reasons. One, we can study the answers from a questionnaire gradually. This makes it easier for us to analyse how the caller experienced the process of using BankID to verify themselves during a phone call and what they thought about the implementation. Two, if we send a questionnaire, they can fill out the questionnaire when they have time and we would interrupt their day as little as possible.

We chose to do interviews to attain more qualitative data as a complement to the quantitative data we got from the questionnaires. The interviews were semi-structured, containing a mix of open and closed questions since we wanted to know how the participants felt about our implementation, both in regards to security and usability. With interviews we can test different methods of authentication and compare them to each other. It also allows us to observe the participants reactions and expressions during the interview. By having interviews, we could acquire answers to our research question: *Which of these models fits the following criteria the best: Ease of use and Risk of stolen identity?*.

Chapter 4

Selection of Models

In this chapter we present seven different models using BankID for authentication during phone calls. We then mention pros and cons for each model, focusing on security and ease of use. After coming up with the models we evaluate them using storyboards and our pros and cons lists to be able to select which models to implement. The selection is not only dependent on the evaluation, but also if it is feasible for us to implement it with our limitations.

After looking into the different models and their pros and cons we found that it was important to select the most suitable models to implement. To make it possible for a reader to make the most suitable choice for their own implementation, we have this chapter as an explanation to our selections.

4.1 Initiating a BankID Authentication Request - Block A

When searching for different models of implementing BankID authentication for phone calls, we started to look at which models exist now that authenticates a user when for example logging into a website or an app. This research and our ideas resulted in seven different ways which could be applied to our case with phone calls. These seven ways are shown in Figure 4.1.

At step 1 in Figure 4.1 someone is calling a phone exchange and a voice plays explaining the options of either pressing 1 to verify their identity with BankID or pressing 2 to continue with the call. If the caller presses 1 there are different ways to initiate the auth request where some involve collecting the caller's PN, in Figure 4.1 they are shown as 3a-3e.

4.1.1 Database

3a is the option of using a database which stores the phone number connected with a PN. This is the same method as mentioned in Section 1.4.1, matching caller-ID on file. In this option there needs to be a database storing the connection which can be problematic since GDPR needs to be taken into account and the company needs to keep the database updated to be able to trust the stored data.

The pros with this model are that the RP already have collected the PNs and the process starts in the background, so the caller does not have to do anything more than open the BankID application. The cons are that the RP must make the connection between a PN and a phone number in advance and if a phone number changes, the PN must be disconnected from the old number and connected to the new one.

If a spoofing attack happens on a number connected with a PN the BankID app will open on the phone of the owner with the PN connected to that phone number. This might not be a problem if the person being attacked know about this type of attack and does not identify themselves without expecting a request.

4.1.2 SMS

The SMS option 3b is when the caller receives an SMS with a link. This link goes to a web page where they can start the BankID authentication process using the current device or by entering their PN so the RP can send an auth request to BankID. This web page follows the basic use case described in Section 2.3.5. Pros with this model are that the caller can call from any phone, and the RP does not have to collect the PN in advance. A con with this model is that the caller must open the SMS application which directs them to another page, start the BankID authentication, then switch to the BankID application to the identification. This is one more application to open for the caller than to just open the BankID app. As mentioned before, people get told not to trust links from emails and SMS since they are easily spoofed and therefore should not be trusted [7]. With this model the agent needs to make sure that the caller trusts the link sent so they can complete the identification.

4.1.3 DTMF

Another approach is to collect the PN by telling the caller to enter it in the keypad 3c. With this model, the caller will dial the number and after pressing 1 in the first step, an automated voice gives instructions to enter their PN in the keypad. The RP collects the number using the DTMF and then sends request to BankID. With this model, the caller has one less application to open than 3b, but still need to enter their PN. In step 1 the caller has pressed 1 so when they are supposed to enter their PN, they have already used the keypad and knows how to do it. Because they enter their PN in the keypad their is no need for any extra application, web pages or databases for the caller to use. The keypad is widely used to enter information so it is a process many callers knows and should therefore not be causing any problems.

After the callers enter their PN and finishes with the hashtag, the number gets read to make sure it is the correct one, if it is not, the caller needs to do the whole process of entering the number again, press hashtag and listen if it is correct that time. Therefore DTMF is user unfriendly and a minor mistake is a large inconvenience for the user.

This is the approach that the ICA Bank is using, explained in Section 2.3.7.

4.1.4 Mobile Phone Application

Model 3d is where the caller has called through a phone app such as the Flow App, because this option was chosen, the Flow app can open up BankID on that

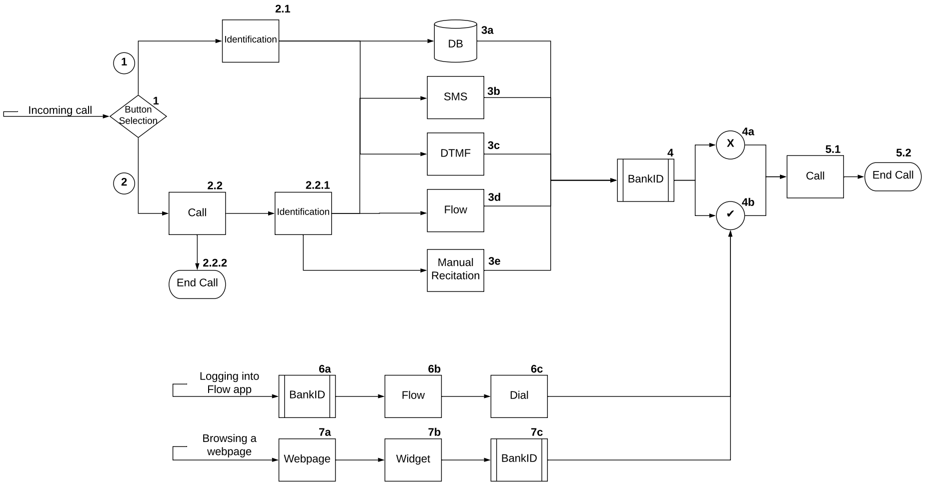

2.1
Identification
3a
DB
1
Incoming call
Button Selection
1
3b
SMS
3c
DTMF
4a
X
4
BankID
5.1
Call
5.2
End Call
2
2.2
Call
2.2.1
Identification
3d
Flow
4b
✓
2.2.2
End Call
Manual Recitation
3e
Logging into Flow app
6a
BankID
6b
Flow
6c
Dial
Browsing a webpage
7a
Webpage
7b
Widget
7c
BankID

Figure 4.1: A flowchart of Block A. Showing how a BankID authentication request can be initiated before or during a phone call.

same phone. To be able to do this, the caller must have the BankID application on the same phone as the Flow App. With this model, the phone number does not have to be connected to the caller's PN and the caller does not have to enter their PN in any way, they only need to open the BankID application to identify themselves. The con with this model is that it only works if the caller calls from the Flow App, and from a phone with the caller's BankID.

If the caller in step 1 press 2 instead, it goes directly to the call without any authentication. If later during the call, the caller needs to identify themselves this can be handled in the same way as when pressing 1 but the agent has to initiate the request manually.

4.1.5 Manual Recitation

In excess of these four models, it can also be done by manual recitation, 3e. This model is when the agent asks the caller to read their PN aloud, the agent enters the PN manually into a system which sends the BankID auth request. Pros with this model are that there is no need for any extra application, web pages or databases for the caller to use. A con is that the agent must enter the PN (in either an integrated web page or an individual one) and can easily hear or enter it wrong. People might also be reluctant to share their PN via phone since it is sensitive information.

This is the model that Soluno uses, explained in Section 2.3.7.

4.1.6 Phone Application Login

There are two more models to identify the caller and this is to do the identifying before dialling the number. The first way to do this is to open the Flow App and when logging in, doing it by using BankID 6a. If BankID approves the identification the caller logs into the Flow App 6b and can make a call. If dialling a number when already logged in using BankID 6c, the call can jump directly to step 4b in Figure 4.1 and the phone call can begin.

One big con with this model is that everyone that calls in needs to have the Flow application, which most do not have. Only people working at a company using Flow might have the app, there is a high probability that their customers do not have the app and do not even know what it is. There would also need to be a rewrite of the current login system, which is no small task.

4.1.7 Website Widget

Another way of logging in with BankID before beginning the phone call is to use a website widget such as the Flow widget. If the caller is using a mobile phone the widget can auto fill the number for the call. It is possible to change it so that if a caller chooses to identify themselves, they can do this before starting the call. The redirection to BankID can be performed in two different ways, either the caller will get redirected to BankID automatically from the widget and when the authentication is completed, continue to the call 7a, 7b, 7c in Figure 4.1. Or this model could use the same link as with SMS 3b, and this link sends the caller to a web page where they get to enter their PN and from there open the BankID application. Since this website has the same functionality as the one needed for SMS, it would be easy to implement this approach if we already have implemented the SMS approach. This first approach has the benefits of not needing to open up BankID manually if they go through the widget and therefore minimize the steps the caller needs to do. Both approaches will, like steps 6a-6d, minimize the call time.

4.1.8 Summary

A summary of all these models pros and cons can be found in Table 4.1 and Table 4.2. Table 4.1 shows security flaws for each model and Table 4.2 shows usability pros and cons for each model. What the tables clearly shows is that the Widget model does not have any cons while Flow only have one pro. Database has 5 pros which is the most of all the models while DTMF have the most cons, 4. If we add 1 for each pro and subtract 1 for each con we receive the sum that is shown in the last row in Table 4.2.

4.2 Showing Authentication Result - Block B

Figure 4.2 shows the different options on how to handle the response from the BankID API.

Table 4.1: A summary of the security flaws for each authentication model using BankID.

	Database	**SMS**	**DTMF**	**Flow**	**Manual Recitation**	**Widget**
Spoofing	X					
Untrustworthy Technology		X				
Phone Number needs to be connected with a PN	X					
Social Engineering					X	

The 2a solution revolves around having a separate web page, not integrated into Flow at all. This is the solution that Soluno has which was mentioned in Section 2.3.7. Because this approach does not connect the web page to Flow it allows for individual deployment and it is not necessary to add or change code in Flow. But that would add another application that requires the agent's focus and humans have problems dividing attention, even in seemingly simple situations [23]. So even if the implementation might be easier it adds problems when in use.

Solution 2b integrates the response into the Flow application, this allows the agents to use the same system as when they are answering the call. Thus, minimizing the amount of divided attention.

In solution 2c the RP sends the data from the BankID response (name, PN etc) to the CRM system where they do the authorization control to make sure the individual calling in has the relevant permissions. This solution depends on the buyers of Flow to develop a CRM system to handle lookup of customers which might be a large-scale project to execute. This would mean that companies buying Flow cannot directly start using it, instead they would have to develop new features and maybe restructure their data.

4.3 Storyboards

We made storyboards for the models we thought were feasible for us to implement. A storyboard is a sketched step-by-step animation of how the process will look like. We did this to be able to understand more of which steps the users of a potential finished prototype, in this case the callers and the agents, would need to do to complete the authentication. By using the storyboards we could confirm some of the pros and cons of the models described in Section 3.3. We will therefore mention some of the pros and cons again and analyse them further.

4.3.1 Manual Recitation

The first storyboard was the model with manual recitation shown in Figure 4.3. When looking at the storyboard, it shows that the caller does not need to open

Table 4.2: A summary of the usability pros and cons for each authentication model using BankID.

	Database	**SMS**	**DTMF**	**Flow**	**Manual Recitation**	**Widget**
Cons						
More apps than BankID to open		X				
User unfriendly			X			
Few have the application				X		
Prone for human errors			X		X	
Long time away from phone call		X	X			
Outdated			X			
Pros						
Happens in the background	X					
Well known		X	X			
One app to open	X		X		X	
Short time away from phone call	X				X	X
Authentication before the call						X
User friendly	X	X				
No need to enter PN	X	X		X		X
Sum	5	1	-2	0	1	3

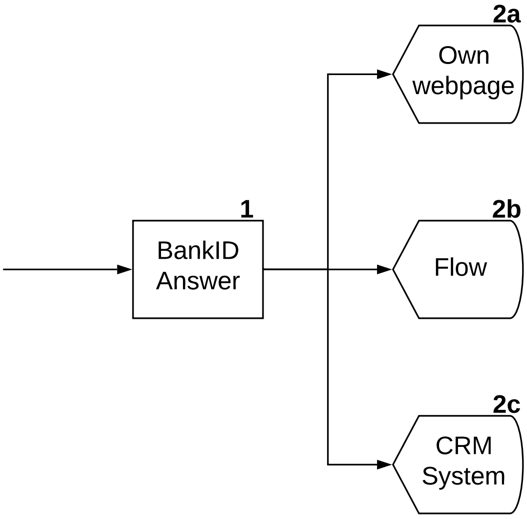


Figure 4.2: A flowchart of Block B. Depicting the different solutions to handle the response from the BankID web service API.

several applications, just read their PN to the agent then open BankID. This makes room for few misunderstandings and mistakes. Even if a mistake or misunderstanding happens, the caller is only away from the phone during the brief time it takes to open up BankID and complete the authentication which makes it possible for a quick correction.

What the storyboard also showed is that the agent needs to be working with two different web pages; Flow where they answer the call and the web page where they enter the PN and receives the result from BankID. The bottom row in Figure 4.3 shows the agent's view where in square 1 they are answering the call in Flow and in square 2 they are entering their PN in the separate web page. Finally, in square 3 they receive the result from the BankID request and must check the resulting name and PN to their own CRM to see if that person is allowed to access the information they ask for.

This model is easy for the caller to understand and carry out, it does not have many steps, and most callers knows how to both read their PN aloud and open the BankID app. On the other hand, the agent has many steps where they accidentally can do something wrong. They need to be able to hear and enter the PN correctly, which are two places mistakes may occur. After these two steps, they receive the answer from the request, now they need to check that this person is allowed to access the information they asked for. To do this they need to compare the name and the PN from the answer to their CRM system. This model needs to trust that the agent does this check every time and not trust that the caller is allowed to access the information just because they authenticated themselves with BankID. In the case of two people having similar names and PNs, the agent needs to realise this and not just assume that the name is right just because it looks similar.

This model's weakest link is the humans that are using it, so every agent needs to be careful and observant to details.

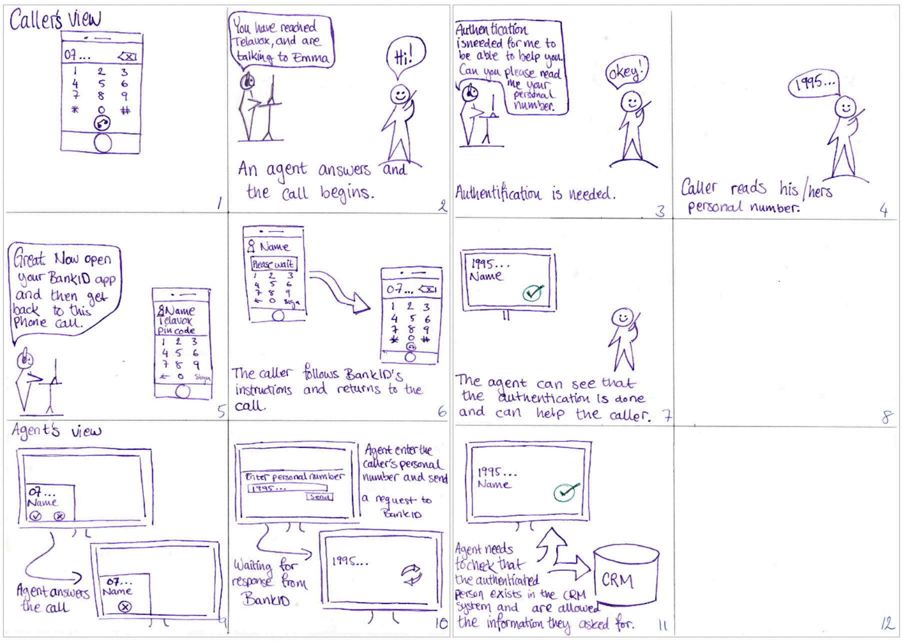

Caller's view
07...
1 2 3
4 5 6
7 8 9
* 0 #
1
You have reached Telavox, and are talking to Emma
Hi!
An agent answers and the call begins.
2
Authentication is needed for me to be able to help you. Can you please read me your personal number.
okey!
Authentification is needed.
3
1995...
Caller reads his/hers personal number.
4
Great Now open your BankID app and then get back to this Phone call.
Name
Telavox
pin code
Sign
5
Name
Please wait
The caller follows BankID's instructions and returns to the call.
6
1995...
Name
The agent can see that the authentication is done and can help the caller.
7
8
Agent's view
07...
Name
Agent answers the call
9
Enter personal number
1995...
Send
Agent enter the caller's personal number and send a request to BankID
Waiting for response from BankID
10
Agent needs to check that the authenticated person exists in the CRM system and are allowed the information they asked for.
CRM
11
12

Figure 4.3: A storyboard for manual recitation with both the caller's and the agent's view.

4.3.2 DTMF

The next storyboard we created was for when the caller is to enter their PN in the keypad, shown in Figure 4.4. For this model there is also no need to open several applications, but the caller needs to open the keypad and enter ten digits plus the hashtag. This adds to the time the caller is away from the call if the caller is not using the speaker or a headset. The caller does need to jump between listening and typing two times, from either 2a-3a or 2b-3b and 4a-5a, which leads to there being more times the caller can miss the start of a message if the caller does not listen quickly enough.

Collecting information with DTMF is something that is common and therefore should not cause any confusion for the caller. With this model, the caller is entering their PN so the risk of the agent hearing or typing it wrong disappears, but the responsibility of typing correctly moves to the caller instead.

With this model, the agent does not need to jump between many different web pages. The agent only wants to receive the response from the BankID request, which can be implemented in Flow. This will make it simpler for the agent since they do not need to switch between many pages. If the caller chooses to complete the authentication before the call the agent's view will look like demonstrated in the bottom row in Figure 4.6.

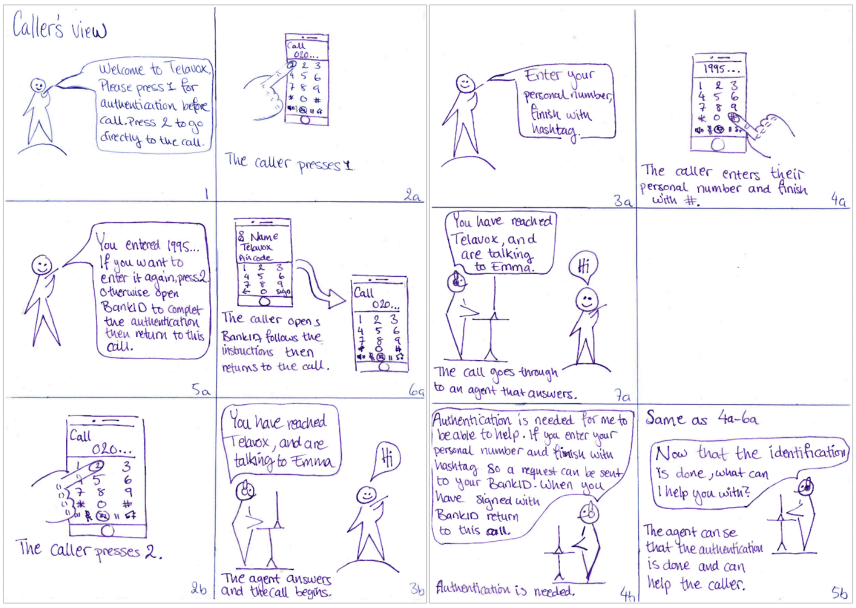

Caller's view
Welcome to Telavox. Please press 1 for authentication before call. Press 2 to go directly to the call.
1
Call 020...
The caller presses 1
2a
Enter your personal number, finish with hashtag.
3a
1995...
The caller enters their personal number and finish with #.
4a
You entered 1995... If you want to enter it again, press 2 otherwise open BankID to complet the authentication then return to this call.
5a
Name Telavox Pin code
The caller opens BankID, follows the instructions then returns to the call.
Call 020...
6a
You have reached Telavox, and are talking to Emma.
Hi
The call goes through to an agent that answers.
7a
Call 020...
The caller presses 2.
2b
You have reached Telavox, and are talking to Emma
Hi
The agent answers and the call begins.
3b
Authentication is needed for me to be able to help. If you enter your personal number and finish with hashtag so a request can be sent to your BankID. When you have signed with BankID return to this call.
Authentication is needed.
4b
Same as 4a-6a
Now that the identification is done, what can I help you with?
The agent can se that the authentication is done and can help the caller.
5b

Figure 4.4: A storyboard for DTMF with two different ways to come to the solution that the caller enters their PN in the keypad on the phone.

4.3.3 SMS

The next storyboard in Figure 4.5 shows a caller receives an SMS with a link to a web page, where they can verify with BankID on their current device or with another device by entering their PN.

With this model the responsibility of entering the PN lies on the caller, the same as with DTMF. A con with this model compared to manual recitation and DTMF is that the caller needs to open more applications than BankID, both the SMS application and a web browser. Because of this, the caller will be away from the call a long time to open a link, enter their PN and then use BankID to complete the authentication. Even though the caller is away from the call, there is only one jumping back and forth between looking at the phone and listening into it. The caller does not have to enter their PN if they have BankID installed on their current device, saving some time and reduces risk for human errors.

A big benefit of this model is that we can easily reuse it. The model where the caller comes from the widget can use the same link as the agent send the caller in this model, it is another way to arrive at the same web page.

Like with DTMF, the agent does not need to jump between pages, because the answer from the request can appear in Flow.

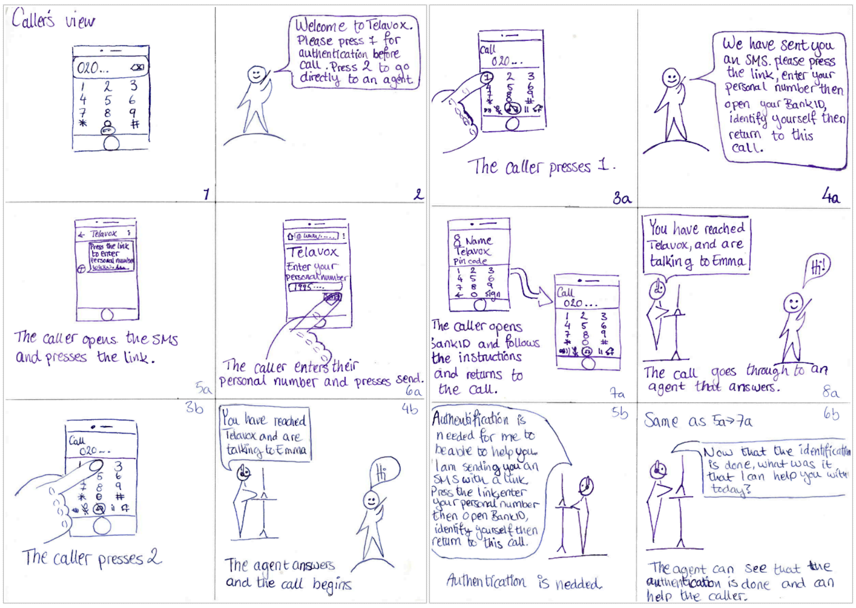

Caller's view
020...
1 2 3
4 5 6
7 8 9
* 0 #
1
Welcome to Telavox. Please press 1 for authentication before call. Press 2 to go directly to an agent.
2
Call
020...
The caller presses 1.
3a
We have sent you an SMS. please press the link, enter your personal number then open your BankID, identify yourself then return to this call.
4a
Telavox
Press the link to enter personal number
The caller opens the SMS and presses the link.
5a
Telavox
Enter your personal number
1995....
The caller enters their personal number and presses send.
6a
Name
Telavox
Pin code
sign
Call
020...
The caller opens BankID and follows the instructions and returns to the call.
7a
You have reached Telavox, and are talking to Emma
Hi!
The call goes through to an agent that answers.
8a
3b
Call
020...
The caller presses 2
4b
You have reached Telavox and are talking to Emma
Hi
The agent answers and the call begins
5b
Authentification is needed for me to be able to help you. I am sending you an SMS with a link. Press the link, enter your personal number then open BankID, identify yourself then return to this call.
Authentication is nedded
6b
Same as 5a→7a
Now that the identification is done, what was it that I can help you with today?
The agent can see that the authentication is done and can help the caller.

Figure 4.5: A storyboard for SMS with two different ways to come to the solution that the caller receives a link via SMS where they can initiate a BankID authentication request.

4.3.4 Database

The weakest link in the previous model showed in different storyboards is the humans using it, the model using database minimizes the risk of human errors. This model is shown in Figure 4.6. Here the caller only needs to press 1, listen to the automated message and then open the BankID app. There is no need to type or recite the PN, but it does as mentioned, require that the PN somehow entered the system beforehand.

This model also requires a minimum amount of work for the agent receiving the call. The agent only needs to look at the icon in the interface to see if the caller completed the verification process, and when the authentication is complete look it up in the CRM system. This model has the fewest steps compared to the other storyboards, shown in Figure 4.6.

Using a database minimises the amount of work required by both the caller and the agent, but the issue with how the caller's PN enters the database is still a problem. The connection between everyone's PN and phone number also needs to be maintained and kept up to date, which is a problem in itself.

4.4 Interesting Models

In this section we will describe some of the models found using the two flowcharts shown in Figure 4.1 and 4.2. These models all stand out in some way.

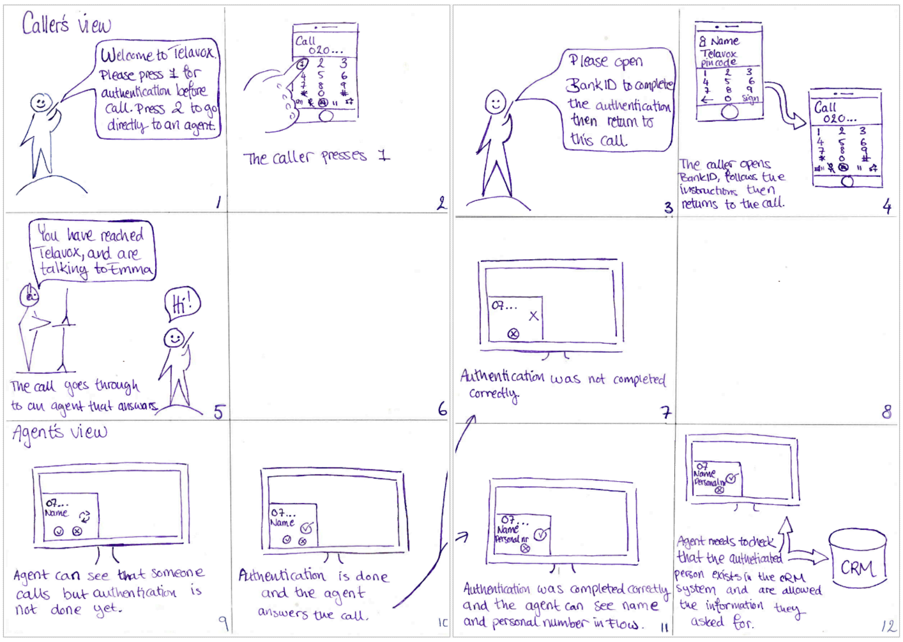

Caller's view
Welcome to Telavox. Please press 1 for authentication before call. Press 2 to go directly to an agent.
1
Call
020...
1 2 3
4 5 6
7 8 9
* 0 #
The caller presses 1
2
Please open BankID to complete the authentication then return to this call.
3
8 Name
Telavox
pin code
1 2 3
4 5 6
7 8 9
← 0 sign
Call
020...
1 2 3
4 5 6
7 8 9
* 0 #
The caller opens BankID, follows the instructions then returns to the call.
4
You have reached Telavox, and are talking to Emma
Hi!
The call goes through to an agent that answers
5
6
07...
X
Authentication was not completed correctly.
7
8
Agent's view
07...
Name
Agent can see that someone calls but authentication is not done yet.
9
07...
Name
Authentication is done and the agent answers the call.
10
07...
Name
Personal nr
Authentication was completed correctly and the agent can see name and personal number in Flow.
11
07
Name
Personal nr
Agent needs to check that the authenticated person exists in the CRM system and are allowed the information they asked for.
CRM
12

Figure 4.6: A storyboard for collecting the PN from a database based on the callers phone number with both the caller's and the agent's view.

4.4.1 The Simplest Model

The model which is the simplest to implement is when a caller manually recites, 3e in Figure 4.1, their PN to an agent who enters the information in to an individual website, 2a in Figure 4.2, and then asks the caller to open their BankID app. After authenticating, the agent can find the result in the same website. The pros with this solution are that it is not necessary to know or learn anything about Flow reducing development time, there is also no need for the company that uses Flow to implement new features. It would also be simple to use, since all the agent needs to do is enter the PN into an input field, click send and verify that the response is okay.

The cons are that the agents handling the calls needs to divide their attention between multiple websites, which may result in reduced performance. There is also no possibility to know the permissions of the caller. The only thing that the agent has verified is that the caller has a BankID connected to the PN delivered during the phone call. Thus, this implementation does not provide any real security features and it requires both the caller and the agent to interact with the system. The agent needs to lookup the PN manually via the CRM system.

4.4.2 The Seamless Model

The most seamless model is by using the database 3a seen in Figure 4.1 to access the PN connected to the phone number together with the CRM system, 2c in Figure 4.2, for verifying the access permissions of the caller. This model minimizes the amount of human interference and therefore reduces the risk of a social engineering attack. It also includes a verification step of the permissions after verifying the identity of the caller, making sure the agent only gives out information the caller is allowed to have.

One of the considerations with this model, and one of the most critical steps, is how the PN is connected to the phone number. Should the callers themselves just enter the information into a form? Should an administrator collect the information and put it into the database? Letting the caller enter their information makes it hard to verify the information but it minimizes the maintenance and effort needed from administrators. On the other hand, letting the registration go through some kind of process to validate the information, for example administrators confirming the information and saving it makes the system more complex. Allowing humans to manually verify the registration might also introduce more risks of errors but the information has gone through some kind of validation which adds more trust for it being correct.

4.4.3 BankID Login Model

One way to authenticate a caller is to have the caller complete the identification before even dialling the number. In Figure 4.1 this type of model is shown as steps 6a-6b-6c-4b-5.1-5.2.

In Flow, you can make calls to other people and the telephone exchange. Instead of doing the authentication while being in the call you can do it when logging into Flow. This would reduce the time in a call because the caller would not need to open up BankID while in the call. The caller can do all these steps before even dialling the number.

Pros with this are the reduced call time and it can also reduce the number of BankID authentication requests needed, which would make this model cheaper. The reason the number of requests would be lower is that the caller can make many calls with only one authentication.

To have the authentication before the call would also reduce the amount of disturbing moments during the call and the agent can feel secure that they are talking to the right person. The agent can also feel confident that sensitive information does not end up in the wrong hands without any authentication during the call. This would also reduce the risk of social engineering attacks because the person calling cannot try to convince someone that they are another person than the person that logged in with BankID.

This model would also make the process of logging in to the application more secure. BankID is a two factored authentication method and therefore more secure than a PIN code or a password. Especially since most people have terrible passwords, for example none of the 10 most common passwords is over 9 characters long and all of them are easy to guess [24].

4.5 Selection of First Implementation

After looking into the different models, we found one model which seemed to be the easiest to implement, the manual recitation model. This is a solution that already exists in other companies and the model is more explained in Section 4.4.1.

This is a functional model even though it has its weaknesses. It is not the most optimal solution, but we chose to start with implementing it to have a proof of concept of using BankID-based authentication for a phone call. We also wanted to compare our next implementation to this one because this model already exists, and we want to see how our next implementation compare to the one that already is in use.

4.6 Selection of Second Implementation

After the first implementation, we analysed the data and knowledge we had collected and discussed with Telavox what they liked and disliked. What we concluded was that the implementation of manual recitation works, and the storyboard was a correct assumption of how the timeline of this approach would look like. With this in mind, and that the first implementation gave the agent all the responsibility of collecting and writing the caller's PN we investigated the remaining six models.

We decided to go with the SMS model. In the SMS the agent sends to the caller, we have a link to the verification web page where the caller can start the BankID authentication process. We chose this approach because we can reuse the web page in other models. The model we implemented is by a link in an SMS, but it could be a link in an email, a link in the widget, or a link from Telavox.se. Because we can use the same verification web page in many ways, we made the decision to make the SMS model our second implementation.

Another reason we chose the SMS model is to make the connection between the caller and a BankID verification. When sending an SMS with a specific link to the person calling, the agent can keep track of that link and see if the caller completed the authentication or not.

Chapter 5

Implementation

An implementation of the selected model can change a lot depending on which system you implement it into and which languages you are writing the implementation in. This chapter will explain how we implemented our selected models, how we integrated them in Flow and explain the problems we encountered and how we solved them. This to help someone that does a similar implementation and encounter the same problems as we did.

5.1 The Manual Recitation Model

We started out by creating a web page in the Flow web application, behind an access wall to make sure that only authenticated people can send the authentication requests. This implementation is shown in Figure 5.1, but only the bottom part of the figure. As Flow already provides the login functionality, we did not have to develop a system of our own. The web page contains a form with only one input taking the caller's PN.

We then connected the front-end using Angular and Java Server Pages (JSP) to make HTTP requests to a route we had defined. After we had implemented the communication between the client and server, we started to implement the integration of the BankID server. This required us to install a certificate and a pair of keys to allow our server to communicate with BankID's server. Since Telavox was not using a key store, this proved to be quite a challenge for us. We had to create a key store and add it to the TLS context. But after looking at similar implementations and a lot of trial and error we managed to connect to BankID's API. We will not go into any details of how the TLS context was setup since it differs a lot depending on the context and the programming language one is working with.

After we set up the connection, we followed the guidelines from BankID on how to start the authentication and collect the result. When implementing the connection between the client and server, Telavox had similar web pages where we could follow the implementation and obtain inspiration from.

5.2 The SMS Model

When we developed the SMS model, we started out by adding one more input field to the already existing agent view, shown in Figure 5.1. The new input field is similar to the one we already have, but it takes a phone number instead. Then we created a verification web page for the caller in Flow, which was not behind an access wall to make it possible for the caller to use it, shown in Figure 5.5. The verification page is for the caller to start the BankID authentication request by themselves and we started out with only having one field where the caller could enter their PN.

At first, the agent had to manually enter the phone number, but it required no reciting from the caller if they were calling from their cell phone, and the caller had to enter their PN manually. We then modified the implementation so the phone number of the caller was automatically filled in if it was a Swedish mobile number. We also implemented a feature making it possible for the caller to use BankID on their current device, which gives them the option not to enter their PN at all.

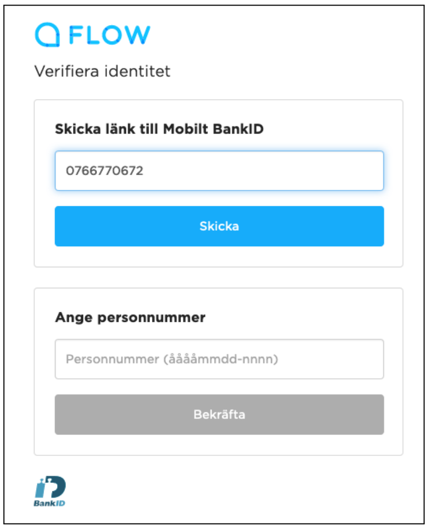
After the agent sends the phone number to our server, we create a token using the symmetric key algorithm; blowfish. Telavox already used this method of encryption in other functionalities and the algorithm is considered secure. We encrypt the phone number concatenated with the current time to make sure the encrypted data string is unique. The phone number is then saved in a cache together with the duration time which we have set to ten minutes to allow mis happenings but still make sure that it can not be used after the call. If the agent for some reason lost connection after starting an authentication process but before it was complete it is possible to reconnect to that process. If a phone number which has a process running is submitted by the agent they will receive a choice between reconnecting to the current active process or to start a new one by sending a new SMS, shown in Figure 5.4

After saving the token to the cache we send an SMS to the caller with a link to the verification page and a token as an URL parameter. During this process the agent sees a loading spinner, shown in Figure 5.2.

When the caller arrives on the page we validate the token before the caller can enter their PN or open BankID on their current device. When the caller's token has been validated and they have started the BankID authentication process they will receive a message telling them to open the BankID application, shown in Figure 5.6. If the caller chose to authenticate using their current device they will barely see this message. After completing the authentication the caller will see a confirmation message, shown in Figure 5.9 and the agent will see the information of the caller that authenticated via the link, shown in Figure 5.3. After a successful verification we invalidate the token used so if the caller would try to use the link again they would see an error message, shown in Figure 5.7. If something else would go wrong for the caller during the process, they will see a generic error message and the option to try again, shown in Figure 5.8.

5.2.1 CRM Integration

What we have found out through the implementation is that both models only work if the agent follows all the thought-out steps and looks up the PN in the CRM system. To make this probability as high as possible, we implemented a button that copies the caller's PN when they are authenticated. This button is there to make it as easy as possible to check whether the caller is authorised to access the information they are asking for or not. If the agent does not check with the CRM system, all the steps taken by both the caller and the agent to authenticate the caller with BankID are pointless.



Verifiera identitet

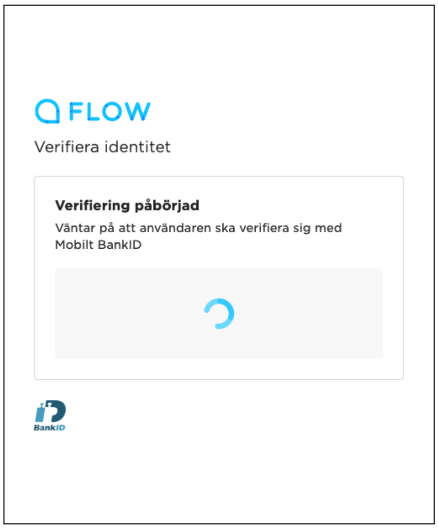
Skicka länk till Mobilt BankID

0766770672

Ange personnummer

Personnummer (ååååmmdd-nnnn)

Figure 5.1: The agent's view before initiating the authentication process.

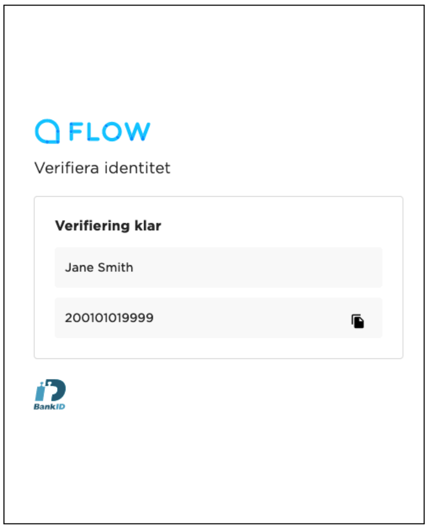


Verifiera identitet

Verifiering påbörjad

Väntar på att användaren ska verifiera sig med Mobilt BankID

Figure 5.2: The agent's view when the authentication process is running.



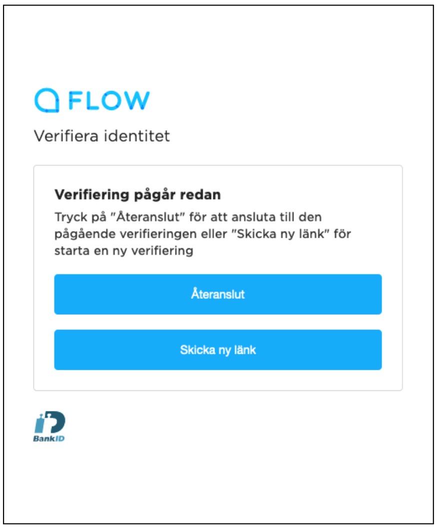
Verifiera identitet

Verifiering klar

Jane Smith

200101019999

Figure 5.3: The agent's view when the authentication was successful.


FLOW

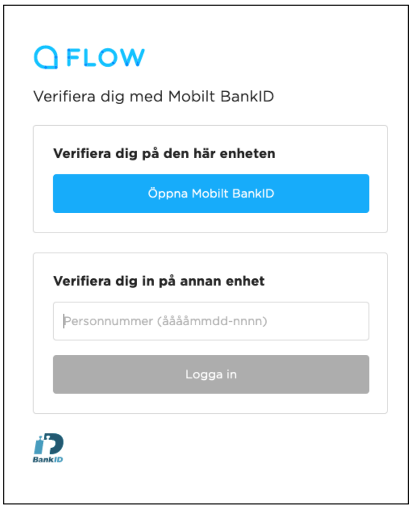
Verifiera identitet

Verifiering pågår redan

Tryck på "Återanslut" för att ansluta till den pågående verifieringen eller "Skicka ny länk" för starta en ny verifiering

Återanslut
Skicka ny länk

Figure 5.4: The agent's view when an authentication process is already running for the phone number entered.


FLOW

Verifiera dig med Mobilt BankID

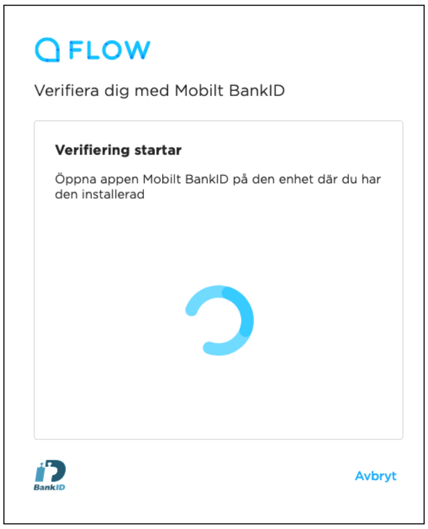
Verifiera dig på den här enheten

Öppna Mobilt BankID

Verifiera dig in på annan enhet

Personnummer (ååååmmdd-nnnn)
Logga in

Figure 5.5: The caller's first view after pressing the link in the SMS the agent sent.

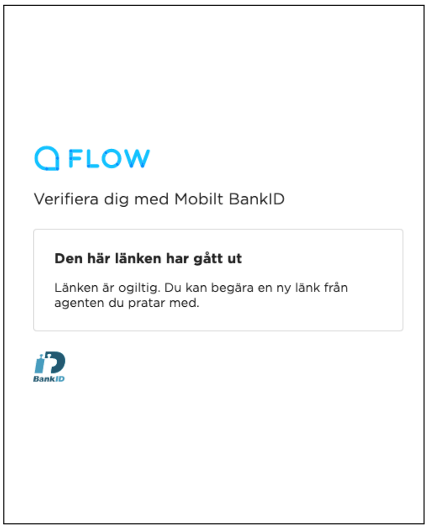


Verifiera dig med Mobilt BankID

Verifiering startar

Öppna appen Mobilt BankID på den enhet där du har den installerad

Figure 5.6: The caller's view when they should open their BankID app.

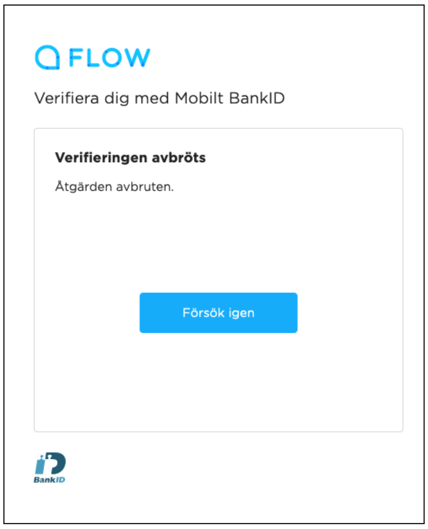


Verifiera dig med Mobilt BankID

Den här länken har gått ut

Länken är ogiltig. Du kan begära en ny länk från agenten du pratar med.

Figure 5.7: The caller's view when their token is already used or old.

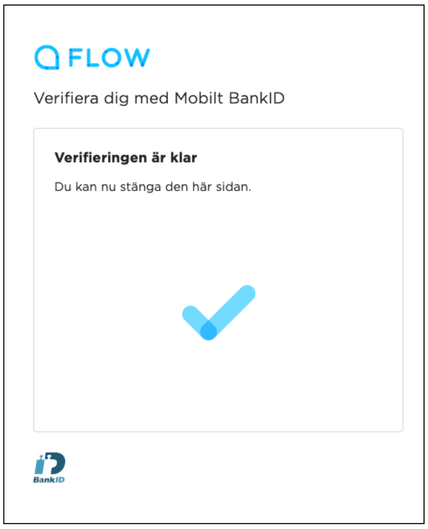


Verifiera dig med Mobilt BankID

Verifieringen avbröts

Åtgärden avbruten.

Figure 5.8: The caller's view when something went wrong.



Verifiera dig med Mobilt BankID

Verifieringen är klar

Du kan nu stänga den här sidan.

Figure 5.9: The caller's view when the authentication was successful and they can go back to the call.

Chapter 6

Evaluation

To evaluate the finished prototype we conducted empirical researches, through questionnaires to agents and callers and interviews with test cases. This chapter will be about how we made the questionnaires, created the cases for the interviews, and why we choose these two methods of empirical research.

6.1 Questionnaires

A perfect structured questionnaire where everyone understands all the questions unequivocal and can answer them the right way will we never be able to create, but it was the goal we aimed for. We followed SCB's advice on how to phrase the questions and what to think about when choosing the questions [8].

6.1.1 Who Receives the Questionnaire

We made the decision to make two questionnaires, one for the agents to answer after they have had a call where they authenticate the caller using BankID, and one questionnaire for the callers who used BankID.

To make it possible for us to answer our research question: *How does the implementation affect the current product according to the criteria: Ease of use?* we asked the caller questions focused on this subject.

6.1.2 Questions

The questionnaire for the callers had to give us information about how secure they thought the process was and how the agent authenticated them; through SMS or manual recitation. We also wanted the questionnaire to be as short as possible to increase the possibility that the caller answers the questionnaire. We ended up with the questions shown in Appendix B, Section B.1.

For the agent's questionnaire we felt that we could have more questions since it is in the interest of the agents to try these models in order to see if it could be something they would like to work with or not. Since the questionnaire to the callers only catches the cases where the authentication was successful, the questions to the agent takes into consideration both the cases where the authentication process was successful and unsuccessful. With the questions to the agents we hope to find out if our model is practical in a real business environment. We came up with the questions shown in Appendix B, Section B.2.

6.1.3 Where to Find the Questionnaires

We decided to make it as simple as possible for both the agent and the caller to find their respective questionnaire since we hoped that it would give us as many answers as possible.

The agent could find the questionnaire on the page where they got the result from the authentication, shown in Figure 6.1. The agents also got an email before they started using our prototype with information on how the process works. In that email, we added the link to the questionnaire if they accidentally closed the window before answering it.

The caller will have a link to the questionnaire on the web page when the authentication is approved, shown in Figure 6.2. We are not showing the caller's questionnaire inline because they are with a high probability using a mobile phone and it is a known problem to show google questionnaires inline for mobile phones. The caller might close the window without looking at it before going back to the call and therefore miss the link to the questionnaire. To prevent the caller from missing the questionnaire we also sent a link to it in an SMS to all the callers that started the verification process after they ended the call. In this SMS we explained why we were sending the SMS and ask them to answer the questionnaire, shown in Figure 6.3.

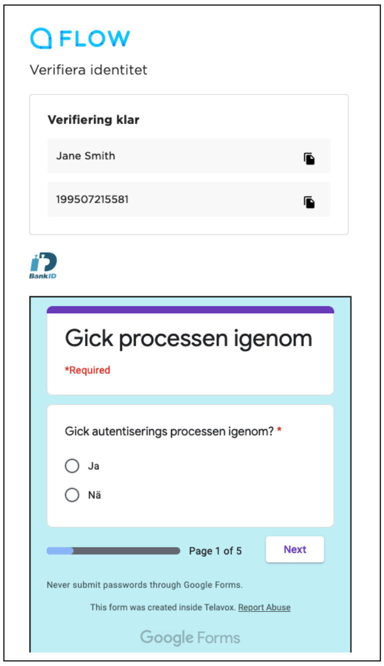
If manual recitation is the chosen method instead of SMS, the caller will never receive the questionnaire. To collect answers from this model as well as the SMS model the agent will receive both their and the caller's questionnaire when the process was successful. The point of this is that the agent can ask the caller the questions aloud and fill in the caller's questionnaire before answering their own.

6.2 Interviews

We decided to conduct interviews to acquire qualitative data of how well our implementations work. Performing interviews also let us observe how the callers react when presented with different methods of verification. We split up the interview in four parts. In the first three parts the participant was acting as a manager of a business that are currently customers to Telavox. They would then call Telavox's customer support (which in this case would be one of us) and try to put in a large order of, for example, mobile phones. We would then verify that they were who they claimed to be in a different way in each of the first three parts. After each part we would ask questions, these questions can be found in Appendix C.1.

In the first part, our method of verification was knowledge-based authentication (KBA) which is described in Section 1.4.1. We chose the following two questions such that they should not take up too much time for someone calling in to be able to answer but also hard enough that it would not be obvious for a fraudster. The questions were:

- How many employees are there currently in your company?



Verifiera identitet

Verifiering klar

Jane Smith

199507215581

Gick processen igenom

*Required

Gick autentiserings processen igenom? *

○ Ja

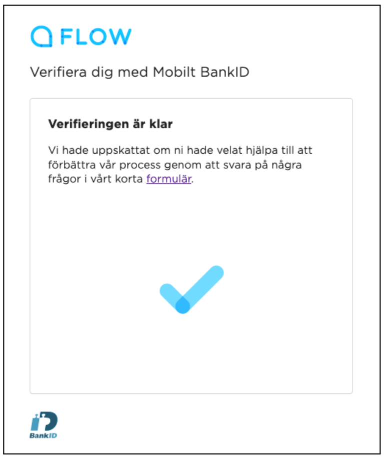
○ Nä

Page 1 of 5

Never submit passwords through Google Forms.

This form was created inside Telavox. Report Abuse

Figure 6.1: Where the agents can find the questionnaire

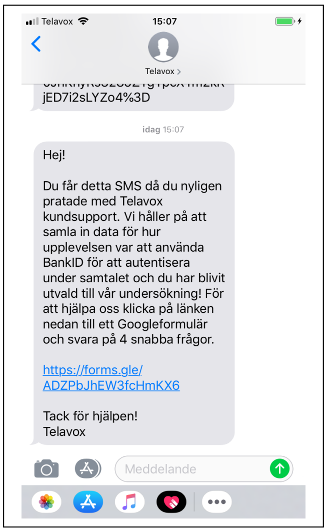


Verifiera dig med Mobilt BankID

Verifieringen är klar

Vi hade uppskattat om ni hade velat hjälpa till att förbättra vår process genom att svara på några frågor i vårt korta formulär.

Figure 6.2: Where the caller can find the questionnaire



jED7i2sLYZo4%3D

idag 15:07

Hej!

Du får detta SMS då du nyligen pratade med Telavox kundsupport. Vi håller på att samla in data för hur upplevelsen var att använda BankID för att autentisera under samtalet och du har blivit utvald till vår undersökning! För att hjälpa oss klicka på länken nedan till ett Googleformulär och svara på 4 snabba frågor.

https://forms.gle/ADZPbJhEW3fcHmKX6

Tack för hjälpen!
Telavox

Figure 6.3: Picture of the SMS we sent out after the call.

- What is the model of your current phone that you have registered to your account?

In the second part we verified the participant using the manual recitation model we implemented, described in Section 5.1.

In the third part we verified the participant using the SMS model we implemented, described in Section 5.2.

Finally, in the fourth part we asked questions where the participant should consider all three parts.

All the questions we asked were to answer at least one of the research questions. In Table 6.1 we have summarised which interview question that is connected to which research question. The focus with the interview is to answer research question two which is: *Which of these models fits the following criteria the best? Ease of use and Risk of stolen identity.*

Table 6.1: The research question which each interview question is related to. The interview questions can be found in Appendix C

Research questions	**Interview question**
Q1. Which models can be used to integrate BankID during phone calls?	**1.**`a,c` **2.**`c,d` **3.**`c,d` **4.**`f`
Q2. Which of these models fits the following criteria the best?	
a. Ease of use	**1.**`b,c`, **2.**`a,b,c` **3.**`a,b,c,e` **4.**`c,d,e,f`
b. Risk of stolen identity	**1.**`a` **2.**`d,e` **3.**`a,d,e,f` **4.**`a,b,d,e,f`

6.3 Target Group

The target group of the caller's questionnaire is customers of Telavox. We decided to have this as our target group instead of random people to make the case as realistic as possible. By having real customers randomly selected we tested the prototype as closely as possible to how it will look when Telavox implements it in the real product.

For the interviews, the target group was different people working at Telavox. We interviewed nine people with different backgrounds, jobs, and experience with BankID. We tried to get a mix of people because in a real case it will be a mix of people using the process.

Chapter 7

Result

In this chapter we will present the results we got from our measurement, tracings when the agents used the prototype, and the result from the interviews.

7.1 Questionnaire

We got ten answers on the questionnaire for agents and three on the questionnaire for the callers.

7.1.1 Agent Questionnaire

The answers we collected from the agents are presented in Appendix D in Figure D.1 to Figure D.5 .

To summarise, all agents completed the authentication with SMS without any problems or questions from the caller. All the authenticated callers had the corrects permissions for what they wanted to do.

7.1.2 Caller Questionnaire

The answers we got from the callers are shown in Appendix D in Figure D.6 to Figure D.10.

To summarise, the answers from the callers displayed that they were all verified through SMS and one third thought about that a link in SMS is not something that you should click on. The fact that it was themselves calling made all the callers feel more secure. Two people thought that the process felt secure and was easy to use. One person thought the process was really difficult to use.

7.2 Tracings on Prototype

The tracings were performed by having the prototype send us an email when an authentication process was started, and if it failed or if it was successful. The email also contained information if the manual recitation or the SMS model was used.

We traced our prototype when it was used for three weeks. During this time, the authentication process was started 57 times and 55 out of those were successful.

Out of the successful, 43 was performed with the SMS model and the caller used BankID on their current device all those times. The manual recitation model was used 12 times.

7.3 Interviews

As explained in Section 6.2 we conducted nine interviews. The short result from these interviews can be found in Table 7.1 and Table 7.2. We asked the participants to explain their answers and those comments are summarised below.

The question “Was it any different that you were the one calling?” was answered by the majority with, “Yes, it feels more secure”. The reasoning was that since they were the one calling, they had already researched and had verified that they were indeed calling Telavox. In addition to this, they also stated that when someone calls you it could be anyone, and not necessarily who they claim to be. The fact that they were the one calling had even larger effect when BankID was involved. The reason behind this was that most of the interview participants had heard of BankID frauds and knew to be careful when signing requests or verifying.

The other questions varied a lot and will be presented thoroughly in each part.

7.3.1 Knowledge Based Authentication

There were a lot of mixed feelings about the security during the knowledge-based authentication. A few of the participants felt that they did not care about the security, they just wanted to be able to order their products as quickly as possible. But most of the participants felt that is was not secure, especially since a fraudster can quite easily find out the answers to these security question. One participant also mentioned that the person calling might not know the answers or might give the wrong answer.

Every participant agreed that this was an effortless way of doing the authentication and order products.

7.3.2 Manual Recitation Model

Continuing with the manual recitation model for authentication almost everyone agreed that it felt more secure than the KBA. But a few of the participants were reluctant to share their PN aloud, they felt that it was a sensitive piece of information. It helped that they were the one calling, otherwise they would have been even more reluctant to share their PN aloud. Almost everyone agreed that this method of authentication would be able to prevent social engineering attacks where a fraudster would pretend to be the caller. They also thought that this method was easy to use.

One thing that stood out when asking the caller to read their PN, almost all of them gave us a questioning look as if they wanted to know if we were serious.

Participant T3 have a * at the question 2e, this is because they answered the question with: Prevent equally as much as other BankID applications.

Table 7.1: Short answers from the interview, the questions were asked after each case.

	T 1	**T 2**	**T 3**	**T 4**	**T 5**	**T 6**	**T 7**	**T 8**	**T 9**
1. KBA									
a. Did the process feel secure?	No	Yes	No	No	No	No	No	No	No
b. Was it any different that you were the one calling?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
c. Was the process easy to use?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2. Manual recitation									
a. How did it feel to read your PN aloud over the phone?	Bad	Bad	Weird	Weird	Bad	Weird	Weird	Bad	Good
b. Was it any different that you were the one calling?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
c. Was the process easy to use?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
d. Did the process feel secure?	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes
e. Do you think this method could prevent social engineering attacks?	No	Yes	No*	Yes	Yes	Yes	Yes	Yes	Yes
3. SMS									
a. People often gets told not to click on links that they get through SMS. Was this something you though about?	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes
b. Was it any different that you were the one calling?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
c. Was the process easy to use?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
d. Did the process feel secure?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
e. Did you use “This device” when open BankID?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
f. Do you think this method could prevent social engineering attacks?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 7.2: Short answers from the interviews asked after the three cases.

	T 1	**T 2**	**T 3**	**T 4**	**T 5**	**T 6**	**T 7**	**T 8**	**T 9**
Summary									
a. Which method do you think is most technical secure?	3	3	3	3	3	2	3	2	3
b. Which method gave you the feeling of being most secure?	3	3	3	3	2	2	3	3	3
c. Which one was the easiest to use?	1	3	1	3	1,2	2	2	2	2
d. With focus on usability and security, which one would you prefer as an authentication method?	3	3	3	3	2	2	3	3	3
e. Would you prefer another authentication method? If yes, which one?	DTMF		Flow			Flow			

7.3.3 SMS Model

The SMS model puts more responsibility on the user and it adds a few steps to the authentication process, but all of the participants felt that it was easy to use, since even though there are more steps it is only a few clicks per step. There is almost no need to do any thinking, which the participants felt was positive and added to the usability of the authentication. Some of the participants thought that it took a long time and felt stressed since the agent were just waiting for them to finish.

When we asked how they felt about clicking the link in the SMS, most of them stated that they thought a little bit about it but since the agent (in this case us) mentioned that they would receive an SMS with a link in it, it instantly felt more secure. Because they made the call, they knew who they were talking to and therefore it felt like less of a risk to click the link. The SMS and the webpage also felt professional, adding to the sense of security.

All the participants felt that this was secure way of authenticating and that it would stop a social engineering attack. One participant also mentioned that there will be a paper trail (the SMS) if there were to be any kind of fraud.

7.3.4 Summary

Most of the participants thought that SMS was the most technical secure model. They motivated it with that they do not need to read their PN aloud and this model has more steps for a fraudster to break to be able to make an attack work. While one of the two participants that thought manual recitation was more secure argued that because SMS had more steps, it was harder to make every step secure and there for was easier to break.

On the question which one they thought gave the feeling of being most secure, a majority answered SMS. They explained their choice with that the SMS model has the least room for human errors, they did not need to give away their PN, and with this model they had the most control, which gave the feeling that the SMS model is most secure.

On the question when we asked which one they would prefer when it comes to both security and usability most answered SMS, not because it was always the one that was the easiest to use but because they ranked security as more important than usability.

Most of the participants would not prefer another method to verify themselves then those we suggested. The ones who did, mentioned the models; DTMF and Flow, which we have described in Section 4.1.

Chapter 8

Discussion

In this chapter we will evaluate and analyse the implementations of the manual recitation and the SMS model. We will then analyse the results from our empirical studies to get an understanding of how well our models performed. After that we analyse the effects our prototype has on a product to be able to answer research question three: *How does the implementation affect the current product according to the criteria: Ease of use and risk of stolen identity?*

8.1 Key Management

After we discussed with our supervisors we decided to try and implement one of the chosen models in production to allow us to test it on the customers of Telavox. This required Telavox to order the public/private key pair from their bank and introduced the problem of key management. The current threat if someone were to steal the private key is quite small since we are only initiating verification requests via BankID. The most damaging attack would involve denial of service on a user's BankID by continuously sending verification requests to that user. This would cause inconvenience for the user and cost Telavox a maximum of a few hundred Swedish crowns before they would detect it.

But if Telavox were to expand the service and require the functionality of initiating sign requests as well, an attacker could make legally binding documents between the user and Telavox. Causing a far greater inconvenience and maybe even legal trouble.

8.2 GDPR

Neither of our models stores the PN entered by the user or the agent. Nor do we store the PN received from the BankID web service API. Since we do not save the information, GDPR barely affects us, but we are still handling sensitive information, so we need to inform the user why they need to enter their PN and how we handle it. If we would have chosen, the database model instead we would have needed to ask all the users for permission to save their PN. We would also have to easily be able to delete and present each entry to ensure accountability and transparency. This would require a lot more work than the two models we chose to implement. The con with not saving the PN is for example if a fraudster obtains sensitive information, we do not save their information and it could be hard to identify who they are afterwards.

8.3 Implementation

According to Agnvall and Lavman's paper in Section 1.3.1 we have followed one of the steps they suggested for more safe use of e-legitimation. They suggested a two-sided authentication which we have incorporated in our solution. The caller authenticates the agent by researching and dialling the number to whom they would like to talk to, and the agent authenticates the caller by using BankID. The caller can also note in the BankID app if it is the correct organisation they are authenticating themselves to, because the caller knows whom they called. If the agent had called the caller, it would not be a two-sided authentication anymore because even if the caller could recognise a number, it is easy to spoof a number and it can therefore not be considered as an authentication. Because we use two-sided authentication we are protected against the attack explained in Section 2.3.9 where the fraudster calls.

According to Nelms [21] a way to authenticate a caller is by using OTP which uses SMS. Our implementation does not send a OTP through SMS, it instead sends a link that only works one time. The cons with OTP are that it is exposed to social engineering and SIM swap attacks and that the agent must trust a phone number. Since the agent sends a link to start the BankID process instead of a password, the agent does not have to trust the phone number, only the result from BankID. Therefore, the SMS method is not exposed to SIM swap attacks, only the social engineering attacks since BankID is not secure from them either.

We chose to not implement the QR code that BankID offers as extra security. This, because we send the link with SMS and can see from the tracings that most of the people that the agents authenticated used the current device which means that they can not scan a QR code with the BankID app.

We did not integrate our solution with the PBX, instead we focused on path two in Figure 4.1, where the caller is authenticated during the call. This was because we did not have time to make our models function automatically or to work with DTMF tones to make the authentication optional.

8.4 Tracings

From the tracings we had on the prototype we can see that SMS was the most used model of the two and the prototype was working almost every time. With this information we conclude that the data we got from the prototype is a complete picture of the SMS model. The manual recitation model was not used as often as the SMS model, but the process was always working. Therefore, even though it was not tested as many times as the SMS model, we conclude that the data from that prototype is valid as well.

8.5 Interviews

We implemented two of the seven models and from the interviews received feedback on both. During the interviews, we instructed the participants to read their PN aloud over the phone. The manual recitation model is dependent on the caller's willingness to do this. Out of the nine people we asked to do this, five of them gave us a questioning look before reading their PN. Eight out of nine of the participants answered that it was either bad or weird to read the PN over the phone. This was not very surprising to us and to make them feel more comfortable with it, and to follow GDPR restrictions, we explained why we required the PN before asking them to read it over the phone. An example of our explanation was: "For us to be able to help you make an order this big we need to make sure that you are who you claim to be. And after that check in the CRM system to see if you have the right permission to make this order. And for us to do this we would like to verify you with BankID and to start the BankID process we need your PN." With this information they understood why they needed to read the PN aloud, but it was still something that they did not feel comfortable doing.

We mention in Section 1.4.2 that many companies warn their costumers not to trust emails and because of ID spoofing you should not trust SMS either. Many of the participants in the interview stated that they trusted the SMS and web page because it felt professional. This is a false security for the caller because we decided that the SMS was going to be from Telavox but we could have decided on anything, for example we could have chosen "Bunny" instead of Telavox. With this information, anyone could send an SMS and make the senders name Telavox, so that should not make the caller feel any more secure. The difference with our SMS compared to a random SMS, that you should not trust, is that the caller has called the agent, not the other way around. Because of this, the caller is more confident they are talking to the right person. When the agent then says that they have sent an SMS to the caller with a link addressed from Telavox, you can trust this SMS more than a random SMS without any context.

Five out of the nine participants did not think that it was a problem to click on the link, while it was only one who did not have a problem reading their PN aloud over the phone. From that result the SMS model makes the caller feel safer when using it.

8.5.1 Social Engineering Attack

Another interesting aspect is if any of the three models used during the interview prevented a social engineering attack. Since none of the participants thought KBA was a secure method, we make the conclusion that it is not secure against social engineering attack either. For the manual recitation and SMS model, the difference was that two participants thought that manual recitation was not secure against the attack while everyone thought SMS was. What one of these two people thought was the difference between the two models, was that because they read their PN aloud during the manual recitation model anyone could overhear it and start a BankID request with their PN. We argue that what even if someone else starts a BankID authentication process using the caller's PN, they still need to verify their identity with BankID. Therefore, if the caller notes who requests an authentication in the BankID app before verifying themselves it is not a problem.

The other participant that said no for manual recitation and yes for SMS was T3. T3 has a * at the question 2e which is the question about social engineering, where they answered the question with: "Prevent equally as much as other BankID applications". Agnvall and Lavman concluded that the only attack that works on BankID is social engineering attacks so if this person knew that, he or she would have thought this model is not secure from social engineering attacks [1].

What we can conclude from the interviews is that most users see BankID as a secure way to authenticate, both against technical attacks and social engineering attacks. We think that Agnvall and Lavman 1.3.1 are correct and BankID is not totally secure from social engineering attacks and this is something the user easily misses. As mentioned in Section 2.1 if you do not treat social engineering attacks seriously, you are an easier target compared to one who does.

BankID is most vulnerable for a social engineering attack when someone calls you and you agree to verify with BankID without looking at what you are verifying yourselves for, see example in Section 2.3.9. But for our prototype the user will be the one calling to a number they have looked up, removing one of the biggest vulnerabilities of BankID.

Our prototype will struggle if the caller refuses to use BankID, maybe because they know that social engineering attacks are common via phone, but from looking at the results from the interviews and questionnaires this does not seem likely.

We noticed during the interviews why social engineering attacks might work. All the participants felt safe because the website looked professional, also their reactions during the interview depended a lot on how sincere we sounded over the phone. This is what fraudsters abuse; it is easy to make a website look professional and to sound sincere. But hopefully awareness of these attacks is spreading. From the results of our interview we could see that it made a difference that the participant was the one calling and some of them would have refused to share their PN or following the link in the SMS if that was not the case. This shows some spread of awareness, but we still think it is important to inform people of these attacks.

From the tracings and interviews we conclude that the SMS model is secure against social engineering attack and while still being easy to use which answers research question 2 (*Which of these models fits the following criteria the best? a. Ease of use. b. Risk of stolen identity (e.g. social engineering)*).

8.6 Questionnaires

We thought that by having real customers test our prototype, the agents at Telavox would use it many times per day. What we quickly found out was that there were few daily use cases where the agents could apply our prototype. This surprised us because we thought that there would be more use cases, for example when callers wanted to order products or get access to PIN codes for their SIM card.

We only got a few responses on the questionnaire from the callers and therefore a small amount of quantitative data. What we could have improved is to have had the process out for testing a longer time so the agents using it could have gotten more cases to test on. This would increase the probability of receiving more answers from the callers. Because of the few answers, we have decided that the data is inconclusive.

But what we could see from the data is that every test we did with the prototype the process has been successful and performed via SMS. From the answers from both the questionnaires, we conclude that the prototype got a positive response.

One of the callers that answered the questionnaire answered that the process was difficult to use. We think this might have been because they misunderstood if 5 was really easy or really hard. We decided to keep it that way anyway to not make the positive answer on the right side for both the questions that were ranked from 1 to 5. Now afterwards, we think that this was an unwise decision and only confused the people answering the questionnaires.

8.7 Effects on Product

Adding new features to an existing product will always make it more complex, both for the users and the people maintaining and developing the product. Our prototype is not an exception. By adding BankID to a product it is required to manage public/private key pairs and certificates, if this already exists in the product the effect of adding BankID is quite small. But if it does not exist before, handling private keys is known to be a hard problem [10]. Especially if your product is running on different hosts that all need access to the private key. Therefore, one of the effects our implementation has on an existing product is the need to manage key and trust stores.

For an organisation to make use of our prototype they need a CRM system where they save the users' PNs, preferably connected to a phone number. The BankID API also returns the name of the user verifying themselves but since names are not unique the PN is the most important piece of information to keep track of. This solution offers the highest security and can give the agent the most confidence that the caller is who they claim and that they have the permission to receive the information they want. But since the PN is sensitive information, it requires particular care according to GDPR, which might lead ot legal issues if one does not comply.

Our prototype will also make the product harder to use if there does not exist any method of authentication previously. Telavox for example, only looked at the number calling in, if it existed in their CRM system that would be sufficient authentication. But with our solution both the caller and the agent are required to perform more actions to complete the authentication. This in return for a more secure authentication and proof of identity from a trusted third party, BankID.

To sum up how our solution affects the current product and to answer research question 3 (*How does the implementation affect the current product according to the criteria: Ease of use and risk of stolen identity*):

- Adds a need to manage public/private key pairs and certificates in order to communicate with the BankID web service API.

- Adds a need to manage PNs to make the most use of BankID, which might be troublesome because of for example GDPR.
- Makes the product harder to use in return for better authentication, reducing risk of stolen identity.

8.8 Improvements

Because of the time limits we did not have time to see if the agents used our implementations correctly. What we would have wanted to do was observations on the agents. By doing observations we could have seen if the agents always checked the person's permissions in the CRM system and used all the functions correctly. For example, if they used the copy paste function instead of writing the caller's name after into the CRM system. We could have performed observations on the agents, but since they used it during such a brief time, we did not feel it was enough time for the agents to become familiar with our prototype. We decided to spend the time we had on conducting interviews instead.

8.9 Future Work

In this thesis we have focused our research on how the Swedish e-ID BankID can be used as authentication for phone calls. And if BankID can potentially stop social engineering attacks targeting companies who can impossibly recognize who is calling in. Further research could focus on different methods of authentication, especially in our time when everyone has a smart phone which allows for more sophisticated methods of authentication.

Our implementations require manual action by the agent, either by asking for the caller's PN or by sending an SMS to the caller. Comparing our models to automatic models (such as the model we described in Section 4.4.2) where the PN is collected through automatic processes before the call could show how users react differently to automated processes and when talking to humans. And if they would be more willing to complete an authentication process when they are talking to a human or when it is automatic.

Our models focus on how to collect the PN from the caller and then shows the result in a separate web page. This puts a lot of responsibility on the agent to properly control the permissions using a CRM system. Research could be made on how you after collecting the PN can automatically get the permissions of the caller and present them to the agent in an intuitive way to minimize risk of human errors.

Chapter 9

Conclusions

In this thesis we have produced seven models of how BankID can be used for authentication during phone calls. We then chose the manual recitation and the SMS models as the ones to implement.

In the manual recitation model, the agent asks the caller to read their PN aloud, the agent then starts the BankID authentication using the PN. When the caller has verified themselves with BankID the agent can then see their PN and name, received from the BankID API.

In the SMS model the agent sends out an SMS to the calling number, this SMS contains a link where the caller can start the BankID authentication process. The agent will see the PN and name when the process is completed.

Advisors and salespeople at Telavox used our prototype, unfortunately they did find few use cases during our time at Telavox and we did therefore receive a small amount of quantitative data.

We then conducted interviews to acquire an answer to research question two: *Which of these models fits the following criteria the best? Ease of use and Risk of stolen identity.* The results showed that our implementation would protect against social engineering attack while still being easy to use.

Our conclusions from comparing the already used manual recitation model to the new SMS model is that the users prefers the SMS model. The users prefer the SMS model even though it might take longer to complete and have more steps than manual recitation, the reason being that they feel like this model is more secure and that they have more control.

The users feel like they have more control in the SMS model since they are performing most of the steps during the authentication process. Compared to the manual recitation model where they only read their PN aloud and then all the responsibility is on the agent to have heard it correctly and to type it in correctly. Therefore, the SMS model is more convenient for both the caller and the agent.

Authenticating a person during a phone call is a hard problem to solve. Phone calls are an old technology were people are used to a fluent experience and adding authentication will always make the experience clunkier. We believe that the SMS models solves the problem well since it is simple and only requires clicks and no typing (if the user selects this device), reducing the risk of human errors while still being a smooth experience. A great next step would be to compare the SMS model to a more automatic model such as the database model which might make the experience smoother.

References

[1] Sebastian Agnvall and George Vetö Lavman. E-legitimationsbedrägerier: Balansgången mellan förtroende och vilseledning, 2019. Student Paper.

[2] Ruth Sara Aguilar-Saven. Business process modelling: Review and framework. *International Journal of production economics*, 90(2):129–149, 2004.

[3] Andreas Lindberg . Ny uppdatering för bank-id ska stoppa de ökande bedrägerierna. `https://www.dn.se/ekonomi/ny-uppdatering-fran-bank-id-ska-stoppa-de-okande-bedragerierna/`.

[4] Andreas Lindberg . Polisen: Bedrägerier med bank-id ett systemhotande problem. `https://www.dn.se/ekonomi/polisen-bedragerier-med-bank-id-ett-systemhotande-problem/`.

[5] BankID. Varför inför bankid avläsning av qr-kod? `https://support.bankid.com/sv/fragor-svar/mobilt-bankid/varfor-infor-bankid-avlasning-av-qr-kod`.

[6] BankID. Bankid relying party guidelines. version 3.2.2, 2019.

[7] Aniello Castiglione, Roberto De Prisco, and Alfredo De Santis. Do you trust your phone? In *International Conference on Electronic Commerce and Web Technologies*, pages 50–61. Springer, 2009.

[8] Statistiska Centralbyrån. Fråga rätt, utveckla, testa, utvärdera och förbättra blanketter, 2001.

[9] Datainspektionen. Om personnummer. `https://www.datainspektionen.se/vagledningar/for-dig-som-privatperson/personnummer/`.

[10] Dawn M. Turner. What is key management? a ciso perspective. `https://www.cryptomathic.com/news-events/blog/what-is-key-management-a-ciso-perspective`.

[11] Agency for Digital Government. Så fungerar e-legitimation. `https://www.e-legitimation.se/safungerarelegitimation.4.769a0b711614b669f295d6.html`.

[12] Michelle Goddard. The eu general data protection regulation (gdpr): European regulation that has a global impact. *International Journal of Market Research*, 59(6):703–705, 2017.

[13] Andreas Halvarsson and Tommy Morin. *Elektroniska signaturer: e-affärer utan elände med identifiering, signering och kryptering.* Studentlitteratur, 2000.

[14] SADTP Kaushalya, RMRSB Randeniya, and ADS Liyanage. An overview of social engineering in the context of information security. In *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pages 1–6. IEEE, 2018.

[15] Lars Dobos. Qr-koden gjorde susen – bankid-bedrägerierna ned med 90 procent. `https://computersweden.idg.se/2.2683/1.721024/qr-koden-gjorde-susen--bankid-bedragerierna-ned-med-90-procent`.

[16] Xin Li, Traci J Hess, and Joseph S Valacich. Why do we trust new technology? a study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems*, 17(1):39–71, 2008.

[17] Malin Wemnell. Statistik bankid – användning och innehav. `https://www.bankid.com/assets/bankid/stats/2019/statistik-2019-07.pdf`.

[18] Malin Wemnell. Statistik bankid–användning och innehav - fördjupning. `https://www.bankid.com/assets/bankid/stats/2018/statistik-2018-12.pdf`.

[19] Ian Mann. *Hacking the Human: Social Engineering Techniques and Security Countermeasures.* Gower Publishing, Ltd., 2012.

[20] Ian Mann. *Hacking the human: social engineering techniques and security countermeasures.* Routledge, 2017.

[21] Terry L Nelms. Caller authentication using mobile devices, 2019.

[22] Netnordic. Bankid-integration. `https://netnordic.se/losningar/telefoni/bankid-integration/`.

[23] Harold Pashler. Dual-task interference in simple tasks: data and theory. *Psychological bulletin*, 116(2):220, 1994.

[24] Rob Picheta, CNN Business. How hackable is your password? `https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html`.

[25] SCB. Befolkningsstatistik, 1:a halvåret 2019. `https://www.scb.se/hitta-statistik/statistik-efter-amne/befolkning/befolkningens-sammansattning/befolkningsstatistik/pong/statistiknyhet/befolkningsstatistik-1a-halvaret-2019/`.

[26] Soluno. Verifiering mobilt bankid. `https://www.soluno.se/foretagstelefoni/kringtjanster/mobilt-bankid/`.

[27] Tan Jin Soon. Qr code. *Synthesis Journal*, 2008:59–78, 2008.

[28] Easy Teams. Mobilt bankid. `https://easytelefoni.se/integrationer/mobilt-bankid/`.

[29] Joel Weise. Public key infrastructure overview. *Sun BluePrints OnLine, August*, pages 1–27, 2001.

[30] Finn Wiedersheim-Paul and Lars Torsten Eriksson. *Att utreda, forska och rapportera.* Almqvist & Wiksell ekomomiförl., 2014.

Appendix A

BankID Web Service API Request and Response Examples

```
POST /rp/v5/auth HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "personalNumber":"190000000000",
    "endUserIp": "194.168.2.25",
}
```

Figure A.1: Example authentication request to the BankID server.

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "orderRef":"131daac9-16c6-4618-beb0-365768f37288",
    "autoStartToken":"7c40b5c9-fa74-49cf-b98c-bfe651f9a7c6"
}
```

Figure A.2: Example answer from the BankID server when sending an authentication request.

```
POST /rp/v5/collect
HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "orderRef":"131daac9-16c6-4618-beb0-365768f37288"
}
```

Figure A.3: Example request sent from the relying party to the BankID server to get status about a authentication request.

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "orderRef":"131daac9-16c6-4618-beb0-365768f37288",
    "status":"pending",
    "hintCode":"userSign"
}
```

Figure A.4: Example response from the BankID server when the status of the authentication is pending.

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "orderRef":"131daac9-16c6-4618-beb0-365768f37288",
    "status":"complete",
    "completionData":{
        "user":{
            "personalNumber":"190000000000",
            "name":"Karl Karlsson",
            "givenName":"Karl",
            "surname":"Karlsson"
        },
        "device":{
            "ipAddress":"192.168.0.1"
        },
        "cert":{
            "notBefore":"1502983274000",
            "notAfter":"1563549674000"
        },
        "signature":"<base64-encoded data>",
        "ocspResponse":"<base64-encoded data>"
    }
}
```

Figure A.5: Example response from the BankID server when the status of the authentication is complete.

Appendix B

Questionnaires for Agents and Callers

B.1 Caller's Questionnaire

1. Were you authenticated through SMS?
    - Yes
    - No
2. People often get told not to click on links that they get through SMS. Was this something you thought about?
    - Yes
    - No
3. Was it any different that you were the one calling?
    - Yes, it made me feel more safe
    - Yes, but it did not make me feel more safe
    - No
4. Is the product easy to use?
    - Really easy 1 2 3 4 5 Really hard
5. Does the product feel safe?
    - Unsafe 1 2 3 4 5 Really Safe
6. Please enter why you felt that way.
7. Do you have any other comments?

B.2 Agent's Questionnaire

B.2.1 Process

1. Did the process go through correctly?

- Yes
  If choosing this one the agent will jump to Section B.2.2
- No
  If choosing this one the agent will jump to Section B.2.5

B.2.2 Verification method

1. How did you verify the user?
    - SMS
      If choosing this one the agent will jump to Section B.2.3
    - Manual recitation
      If choosing this one the agent will jump to Section B.2.4

B.2.3 SMS

1. Did you face any problems?
    - Yes
    - No
2. If yes, what type of problems?
3. Was the person authorised for the information they asked for?
    - Yes
    - No
4. Did you get any question from the caller during the process?
    - Yes
    - No
5. If yes, what was the questions about?

B.2.4 Manual recitation

1. Did you face any problems?
    - Yes
    - No
2. If yes, what type of problems?
3. Was the person authorised for the information they asked for?
    - Yes
    - No
4. Did you get any question from the caller during the process?
    - Yes
    - No
5. If yes, what was the questions about?

B.2.5 Unsuccessful process

1. How did you verify the user?
    - SMS
    - Manual recitation
2. What was in the way of having the process go through correctly?
3. Was the problem in the short guide?
    - Yes
    - No
4. If yes, did the short guide help?
    - Yes
    - No
5. What did you do when the process did not go through?

Appendix C

Interview Questions

C.1 Interview Questions

1. Knowledge Based Authentication (KBA)
    a. Did the process feel secure?
    b. Was it any different that you were the one calling?
    c. Was the process easy to use?
2. Manual Recitation
    a. How did it feel to read your PN over the phone?
    b. Was it any different that you were the one calling?
    c. Was the process easy to use?
    d. How secure did the process feel?
    e. Do you think this method could prevent social engineering attacks?
3. SMS
    a. People often gets told not to click on links that they get through SMS. Was this something you thought about?
    b. Was it any different that you were the one calling?
    c. Was the process easy to use?
    d. How secure did the process feel?
    e. Did you use “This device” to open BankID?
    f. Do you think this method could prevent social engineering attacks?
4. After All Cases
    a. Which method do you think is the most technical secure?
    b. Which method gave you the feeling of being most secure?
    c. Which one was the easiest to use?
    d. With focus on usability and security, which one would you prefer as an authentication method?
    e. Would you prefer another authentication method? If yes, which one?
    f. Do you think this method could prevent social engineering attacks?

Appendix D

Results from the Questionnaires

D.1 Agent Questionnaire

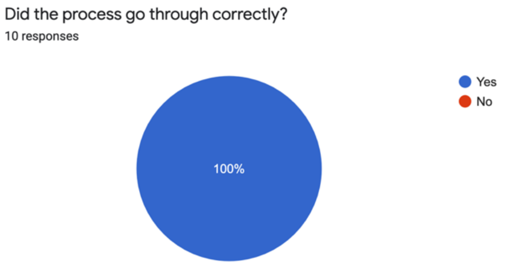


Figure D.1: Responses on question one from the agent's questionnaire.

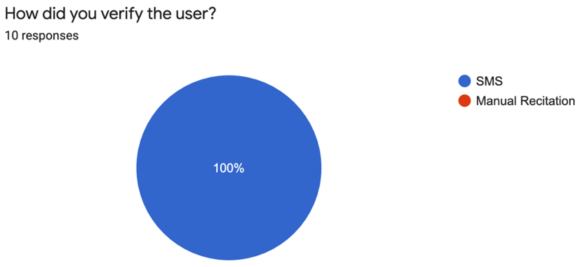


Figure D.2: Responses on question two from the agent's questionnaire.

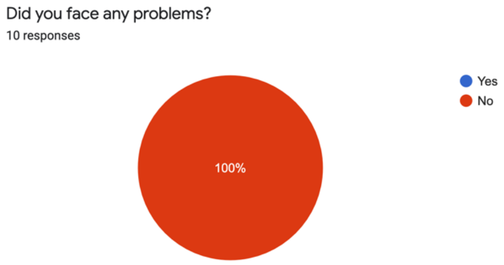


Figure D.3: Responses on question three from the agent's questionnaire.

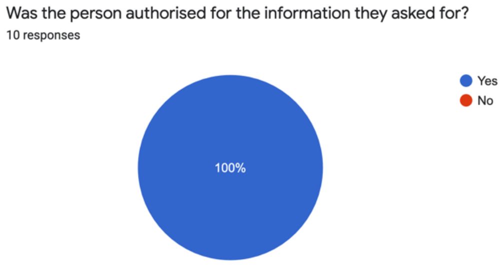


Figure D.4: Responses on question four from the agent's questionnaire.

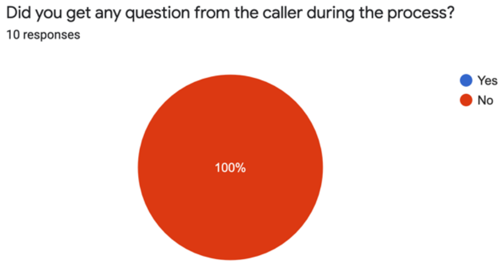


Figure D.5: Responses on question five from the agent's questionnaire.

D.2 Caller Questionnaire

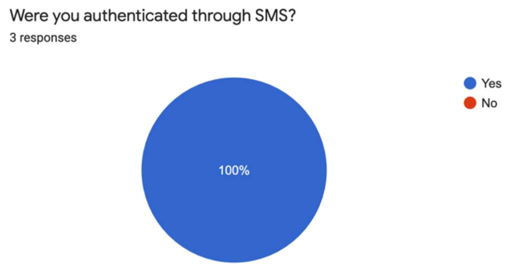


Figure D.6: Responses on question one from the caller's questionnaire.

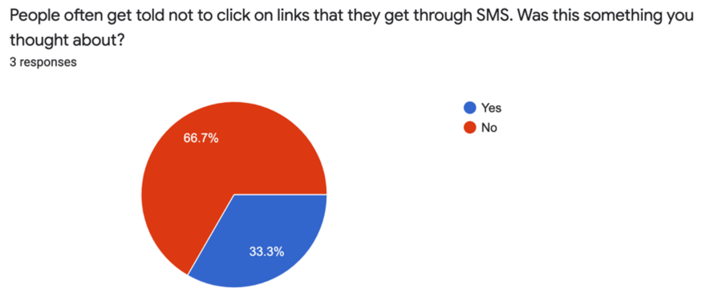


Figure D.7: Responses on question two from the caller's questionnaire.

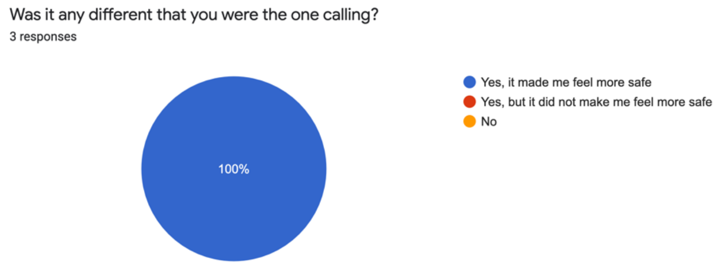


Figure D.8: Responses on question three from the caller's questionnaire.

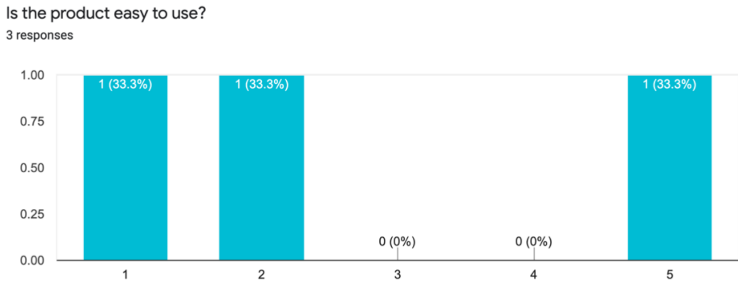


Figure D.9: Responses on question four from the caller's questionnaire.

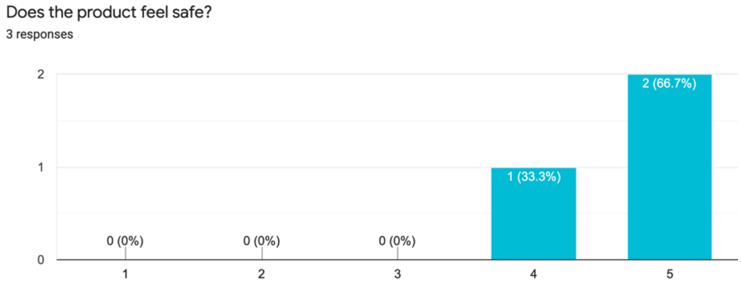


Figure D.10: Responses on question five from the caller's questionnaire.

Printed by Tryckeriet i E-huset, Lund 2020

LUND
UNIVERSITY

Series of Master's theses
Department of Electrical and Information Technology
LU/LTH-EIT 2020-741
http://www.eit.lth.se