Authentication for Phone Calls, Why is it so Different?

Anton Göransson & Emma Asklund

20 januari 2020

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.