Nordea in Finland achieving PSD2 compliancy with future proof SCA

Nordea in Finland achieving PSD2 compliancy with future proof SCA

Banking & Payment Services

How Nordea Finland managed to achieve the best match between user experience and security thanks to out-of-band mobile authentication for smartphone users, completed with hardware based authentication tokens for non-mobile users.

Today the major challenge for the banks in Europe is to find a balance between compliancy, stronger regulations, smoother user experiences and battling ever-complexing fraud. Understanding the landscape of digital banking authentication, as also referred to as SCA (strong customer authentication), is quite complex as security vendors have all proposed their own methods and ways of helping banks to achieve compliancy, and even though it brings options onto the table, it does not necessarily make the puzzle the banks have to face any easier.

In Finland, the biggest bank in the market, Nordea has decided to tackle this challenge by deploying out-of-band mobile solution which bundles top-of-the-line security with a superior user experience for smartphone users. For their non-mobile customers they complemented the offer with hardware authentication tokens. This way they are able to cover 100% of their customer base with the highest level of security and convenience. This case study demonstrates how Thales helped them reach their goals.

Moving from static one-time-passwords to the era of dynamic linking

In Finland, all of the banks have used static lists with one-time-passwords (also known as the code cards) for years in order to provide authentication for their online banking services -- as well as for national online identification purposes. Limited variations in the implementation between the banks have occurred, but looking at the bigger picture, the field of SCA has traditionally been a very manual and static operation for the end-users forcing them to carry the OTP list with them, find the next free code and manually enter it on the website. This clearly has significant user experience limitations, but more importantly it definitely is not a PSD2 compliant level of SCA. Hence, a decision was needed to be made regarding how to replace these lists. Even though this change posed a challenge, it is also an opportunity to change things for something much better! And that's the route what Nordea decided to take: not just a little tweak here and there to reach compliancy, but a complete overhaul once and for all to establish a long term solution reaching beyond simple compliancy.

With the new methods of SCA that Nordea decided to use, they have built-in support for truly strong multi-factor authentication and dynamic linking filling the requirements of PSD2 in a very user friendly and effective way.

Introducing out-of-band mobile authentication and hardware tokens deployed to over one million users in Finland

Identifying yourself for online services, including your online and mobile banking, could not be easier than receiving a request on your smartphone simply asking you to enter your PIN code to authenticate. It's a walk in the park – no more memorizing of long passwords, no manual type-in of secret codes in multiple windows, and no interruption in the usage flow. This is what Nordea's mobile authenticator is all about. And it covers the majority of the user base. But a bank who really cares about their consumers should not provide one solution for all, but instead have it tailored per user segment. This is why Nordea also opted for a hardware token for their non-mobile users, made available in two different formats: one small and easy-to-carry token for the majority of non-mobile users as well as a larger hardware token with a big screen and voice feedback support to cater to user segments with special needs. With this selection of mobile and physical hardware tokens, Nordea is able to address all the needs of their various user groups -- and replace the previous static OTP lists with style and ambition.

Nordea's new authentication methods, smartphone based authentication applications and physical hardware tokens, are already now in use by over one million customers. Nordea was the first bank to introduce smartphone-based PSD2 compliant authentication methods in Finland.

> "Replacing paper password cards with mobile authentication solution has made abuse of the authentication method nearly impossible. This has reduced phishing attempts against Nordea customers significantly"
>
> **Mr. Jani Eloranta, Vice President of Consumer Services at Nordea**
>
> Nordea

Significant reduction in fraud achieved

Phishing messages, which try to retrieve banking information from Finnish banking customers, are very common. Attempts targeted to Nordea customers have however decreased significantly thanks to the popularity of these new authentication methods.

By the end of 2017 and in the beginning of 2018 Nordea customers were a target for fraudsters but since February 2018--when the new methods started to have a significant user base--the attempts have decreased significantly. This is in sharp contrast to the general trend, as phishing attempts are a regular and on-going problem in Finland, and have remained high also throughout 2018

The benefit of Nordea's new SCA method is that fraudsters do not get access to the customer's net bank via user ID and PIN code unless they have a device, either a smartphone with Code App (application including user's authentication credentials) or hardware authentication token. I.e. highly unlikely, if not to say impossible.

> "Our smartphone based Code App and our physical Code Tokens are absolutely the safest methods to use mobile and online bank services, as well as to authenticate to other services"
>
> **Mr. Jani Eloranta, Vice President of Consumer Services at Nordea**

THALES

> Thalesgroup.com <

© Thales 2020. Photos credit: Gettyimages - January 2020 - Design: Jubemo