OneSpan

CASE STUDY

Bank of Cyprus

ENHANCING CUSTOMER EXPERIENCE WITH SOFTWARE AUTHENTICATION AND PSD2-COMPLIANT DYNAMIC LINKING

BUSINESS OBJECTIVES

The Challenge

- Implement software authentication to meet the needs of customers transacting through the mobile channel
- Comply with PSD2's dynamic linking requirement without impacting the CX

The Solution

Used the OneSpan Mobile Security Suite set of SDKs to integrate:

- Software authentication into the Bank of Cyprus mobile app (including Touch ID and Face ID)
- Cronto® technology for authenticating financial transactions

The Results

- High customer satisfaction
- Fully compliant with PSD2
- "We brought in the best security to help our customers feel confident their banking applications and financial transactions are protected."

Bank of Cyprus Group is the leading banking and financial services group in Cyprus. The bank provides a wide range of financial products and services, including retail and commercial banking, investment banking, and insurance. The bank serves customers through the 1Bank Internet banking portal, the Bank of Cyprus mobile banking app, more than 120 branches in Cyprus, a number of subsidiaries and Representative Offices in Moscow and Saint Petersburg in Russia, Kiev in Ukraine, and Beijing in China.

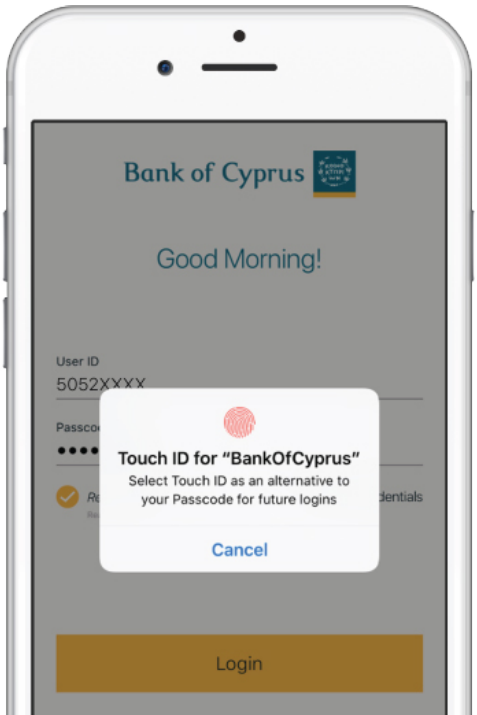
The Bank of Cyprus had distributed OneSpan's hardware tokens to their customer base for years. However, as customers shift to mobile transactions, the bank implemented software authentication and transaction-specific one-time passcodes (OTP) in compliance with the revised Payment Services Directive (PSD2).

The Challenge

Within the bank's Digital Service Channels division, Toula Efthymiadou leads the Business Solutions Department of the Digital Service Channels. She manages business development for the online banking, mobile app, and ATM channels. She is also responsible for the customer authentication technology, and has been a OneSpan customer for 10 years.

"In early 2016, we started looking for alternatives to the OneSpan Digipass® hardware devices, mainly because of the upcoming PSD2 requirements for Internet payments. We also felt that the hardware devices were no longer a modern approach for generating OTPs and doing transaction signing."

Because of their hardware authenticators, Bank of Cyprus was already compliant with the two-factor authentication requirement for account login. However, the



SHARE THIS

bank lacked software authentication capability. With approximately half of all digital banking transactions happening through mobile devices, this had become a more pressing need.

The hardware authenticators had become problematic for some customers. The bank needed to offer an easier and more convenient authentication mechanism where customers no longer had to carry their hardware device(s) around with them – and no longer need to replace them due to battery expiration or heat exposure. For example, with the hot temperatures in Cyprus, hardware authenticators left inside a car in the summer will malfunction.

The challenge for this bank was not replacing the hardware devices with software authentication. The real question was how to comply with one of the key requirements in PSD2: dynamic linking. The requirement to perform dynamic linking (also known as transaction signing) to authenticate a financial transaction is one of the most discussed requirements of the PSD2 Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC).

Because the RTS is technology neutral, it does not prescribe a specific method for implementing dynamic linking. However, the RTS does specify that in the case of a payment transaction, the authentication code must be dynamically linked to the amount and payee, meaning that this code must change if either the amount or the payee is changed during the transaction. Additionally, payment information needs to be exchanged via a secure channel, and must be clearly shown to the user.

European legislators introduced the dynamic linking requirement to counter Man-in-the-middle attacks, where a hacker alters the details of a transaction after the payer authenticates the transaction. Such an attack could change a genuine transfer of 100 Euro to a friend, into a rogue transfer of 1000 Euro to an imposter – without the payer noticing. The regulation intends to avoid social engineering attacks, where a payer is convinced to authenticate data they do not understand, and that later turns out to represent a fraudulent transaction.

Key Requirements

The team knew that they needed to approach PSD2 not merely from a compliance point of view – they also had to optimize the user experience. Doing so meant avoiding a scenario where mobile-first customers would have to toggle back-and-forth between the Bank of Cyprus app and a separate authenticator app.

“From the day we wrote down the functional specifications with the cooperation of the bank’s IT Department and guidance from the bank’s Information Security Department, as well as other departments of the bank, the top requirement was that the software authenticator be fully integrated with the Bank of Cyprus mobile app. Offering a seamless customer experience was key. It was critical that PSD2 compliance not impose a burden on the customer.”

“On the business side, we cooperate very closely with the Information Security department. Once we brought the integrated option to the table, they were convinced.”

The bank also wanted only one presence on the app stores. “We didn’t want to confuse customers with multiple applications,” Toula explains.

The bank determined that they would need the ability to turn off app-to-app communication because multiple users may share the same device. This was very important because in Cyprus, customers tend to share devices. So it was important to not expose functionality that would not be available to the user. “For example, if someone was using a family device for their banking and their personal authenticator was not the one installed on the device, that user should not see the app-to-app option.”

Finally, the bank wanted to source the solution from a single vendor, if possible – one with a proven track record for PSD2 compliance.

> It was very important to have a technology partner with extensive PSD2 expertise.
>
> OneSpan’s support was given to us as a business owner, but they also provided answers to Information Security and even our legal department. OneSpan was very aware of the legal aspects, as well as the aspects that had the potential to affect the customer.”
>
> **Toula Efthymiadou**
> Head Business Solutions – Digital Service Channels, Bank of Cyprus

The Solution

After several consultations on the PSD2 RTS and demonstrations that confirmed OneSpan’s solutions complied with all requirements, the Bank of Cyprus selected OneSpan’s software authentication, as well as the push notifications option and Cronto® solution – all integrated through the SDKs in the OneSpan Mobile Security Suite.

For account login and dynamic linking, the bank decided to introduce software authentication integrated directly into the Bank of Cyprus mobile banking app. For customers who do not use the mobile banking app but still make online payments, the bank offers the ability to receive the OTP authentication code via SMS (online) or scan a Cronto code (offline).

Cronto technology uses a colored cryptogram that represents the encrypted transaction data. When the user wants to initiate a transaction, they:

1. Enter the payment data into the online banking application in the browser. The banking server then generates the colored cryptogram from the payment data and displays it in the browser.
2. Scan the cryptogram using the camera of their mobile device. The device decodes the cryptogram, decrypts the payment data, and shows it to the user as clear text.
3. Authenticate to their device, and it calculates the authentication code over the payment data using a cryptographic key stored on the device.

(Note: Unlike other solutions, a Cronto cryptogram can only be read by an authorized user's authorized device. The code cannot be read by just any device.)

Enter the payment data on your web browser...

...scan the Cronto image with your phone

...check the plain-text payment info and use a unique secure number to authorize the payment.

This approach meets all dynamic linking requirements outlined in the Regulatory Technical Standards.

"It was very important to have a technology partner with extensive PSD2 expertise," says Toula. "The OneSpan PSD2 expert came to Cyprus and answered all of our questions. There were a few questions he couldn't answer, but he maintained communication with us and introduced us to someone in the European Banking Authority (EBA). We exchanged emails with the EBA, and all issues were resolved."

Implementation

"We anticipated a long implementation because on the business side, we put together a functional specifications document of 100 pages. It was very detailed and explained step-by-step exactly what we wanted the customer to experience in every scenario."

The bank outsourced the integration with the mobile banking app and the IT team handled everything else. The IT team prioritized this project as high and started working on it intensively. As a result, the project went live (in pilot) in three months (October 2016 – January 2017).

"Three months from the start of implementation to the go-live. We were amazed to be able to go live so quickly," Toula says.

Activation

"For a customer to understand how to protect their financial transactions with the dynamic linking authentication code, they only need to see a demo once. After that, it's piece of cake. However, to understand how you would set up the software authentication on your device, we thought it was appropriate to have a video to guide customers," says Toula.

The activation is a two-step process:

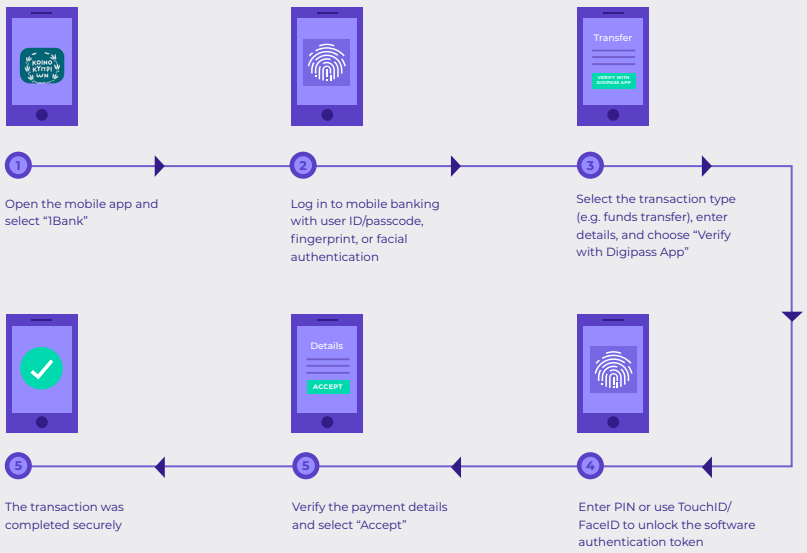
1. First, the customer purchases a software authentication token (to cover costs, the Bank of Cyprus provides it at a very low cost). As soon as a customer has purchased they receive an SMS with the token's serial numb er. They then enter the serial number into the Bank of Cyprus mobile app. That triggers an SMS with an activation code, which the customer also enters into the bank's mobile app. Finally, the customer is prompted to create their PIN or to enable the use of TouchID / FaceID for unlocking the software authentication token. The customer can repeat this process to set up the same serial number on any number of additional devices, free of charge.
2. The customer must now activate the token. This step essentially tells the bank that the customer is abandoning their hardware authenticator and switching to the integrated software authentication on their mobile phone or tablet. It takes about three minutes to complete this step. Customers navigate through the Internet banking portal to complete the process. It is self-serve and customers can do it online 24/7.

"Most customers are able to get through it on their own with no support. Tech-savvy users quickly understand that it's a two-step process and can do it easily. Customers who are not familiar with technology need some assistance. But once they know where to go on our Internet banking to do the activation, they are able to do it."

> With OneSpan's help, we were able to meet the European Banking Authority's strong customer authentication requirements, while at the same time enhancing security and improving the online and mobile banking experience for our customers. By integrating OneSpan's solutions, we brought in the best security to help our customers feel confident their banking applications and financial transactions are protected."
>
> **Charis Pouangare**
> Director Consumer & SME Banking, Bank of Cyprus

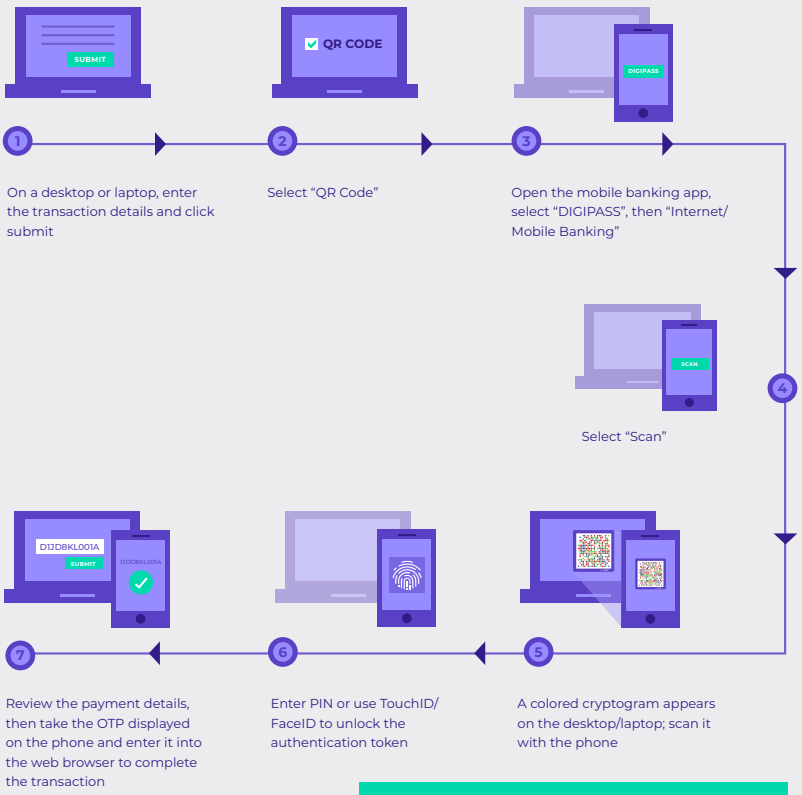
Sample User Flows

AUTHENTICATING A PAYMENT MADE THROUGH THE BANK'S MOBILE APP



See the Full Process on Video

AUTHENTICATING A PAYMENT OFFLINE USING ONESPAN'S CRONTO TECHNOLOGY



See the Full Process on Video

If the user does not have Internet access, they can scan the Cronto code.

"The majority of users prefer Cronto. This is because data plans in Cyprus are very expensive and most people have their mobile data switched off. Because we didn't want customers to incur additional charges with Cronto, we've implemented it offline only," says Toula.

Adoption

"Usage of the integrated authentication is at 30 – 40% to date. The people who have purchased it don't want to go back to using a hardware device. Once they try the software authentication, they are very comfortable. It's seamless and very easy to use."

While the bank recommends that customers replace their hardware tokens with software authentication, many transactions are still signed (i.e., dynamically linked) using the OTP from hardware authenticators.

"Mobile app usage is catching up, but the first customers using the software method are the tech-savvy segment," says Toula.

"From customer feedback through the call center, private individuals prefer the integrated software authentication experience. Overall, in terms of highest adoption, the software authentication is most preferred, followed by the Cronto code."

Training Staff was Key to Adoption

When the bank went live, they published a series of demo videos to help customers understand how to set up the software authentication token on their mobile device and how to use it.

The bank used the same videos for training purposes with call center and branch staff, so they could gain confidence with the new technology and explain it to customers. Because most customers prefer to call the call center for assistance rather than visit the branch, the bank focused primarily on training the call center. The bank piloted the solutions for a week with call center staff. That gave staff the opportunity to get accustomed to the technology and prepare to provide customer support.

The Benefits

Customers perceive the Bank of Cyprus as modern because the bank is enabling technologies like Touch ID/FaceID. "It's things like having Touch ID/FaceID on the device that reinforces Bank of Cyprus as being a leader in the market. The software authentication also enhanced this perception. When we introduced it, we received positive comments from customers. Having new, modern applications and technology is a plus for customer loyalty."

"It was an advantage for us to be the first bank in Cyprus to offer an app as an alternative to the hardware authenticators," says Toula. "Customers no longer have to carry around hardware devices when doing their transactions – and the bank makes it easy for customers to purchase the integrated software authentication token online, provided that they had a hardware authenticator in the first place. The flexibility to purchase and activate online was "another plus for the customer experience, because offering the convenience of a self-service approach is much better than requiring a visit to the branch."

The bank also cut costs because staff no longer need to manually assign and mail hardware to customers.

"We're very satisfied with the OneSpan products and support," says Toula. "If there is an issue, OneSpan responds quickly to remedy the problem. OneSpan's support is fast and it has been for years now. Although our IT team goes to OneSpan whenever they have an issue, as business owners we maintain close contact with our account manager, and they respond very quickly. I've worked with several vendors, but I don't have as good a relationship with them as with the OneSpan representatives."

"My best advice is to go with a vendor that delivers – and OneSpan is definitely a company that delivers."

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to f raud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com

Last Update April 2019