OneSpan

CASE STUDY

BANK SWITCHES FROM HARDWARE TO SOFTWARE AUTHENTICATION

EXECUTIVE SUMMARY

Business Objective

- Upgrade customer authentication technology in the online and mobile channels

The Problem

- Relying on hardware devices alone did not shield customers or the bank's mobile app from fraud
- Multi-password system frustrated customers, generated helpdesk traffic

Results

- Full compliance with new regulations
- Positive feedback from customers
- Reduced helpdesk traffic and fewer hardware devices to manage
- To date, 30% of customers have been migrated

This bank focuses heavily on innovation and technology to provide a trusted customer experience that balances online and mobile security with ease of use.

In 2016, the bank launched a project to offer customers enhanced authentication, including smartphone-based secure authentication technology for mobile transactions. By integrating best-of-breed authentication directly into their mobile banking app and website, the bank has strengthened security, met new regulatory requirements, and cut costs related to issuing and supporting hardware authentication devices.

The Challenge

This bank was under pressure to upgrade their authentication technology. While the bank's customers were already using a different vendor's one-time password (OTP) devices and passwords, the bank needed to implement stronger authentication to comply with new regulatory requirements.

Compliance was not the only challenge. Three other concerns added urgency to upgrade:

Soon-to-expire hardware tokens: One-third of all OTP generators used by customers were just months from expiring.

Customer experience: The bank was still using a multi-password system. Customers authenticated with their OTP device in combination with three passwords – but it was difficult to remember three different passwords. Frustration was building; it was becoming increasingly important to simplify the authentication experience because customers who forgot their passwords couldn't make payments or do trades.

Reissuing passwords was costly: The multi-password method generated a heavy workload for the helpdesk. Forgotten passwords triggered a manual password reset process – consuming valuable helpdesk time. Eliminating this could drive significant savings.

Customer Survey

For years, the bank had provided customers with traditional hardware tokens. However, innovation in the world of mobile security gave the bank new options, namely software authentication for online transactions.

The bank developed a cost analysis to compare the two authentication methods. While the analysis remains confidential, "It was clear that from a cost perspective, using only hardware was not an option," says the Project Manager. Introducing software authentication would provide stronger protection for mobile customers, while cutting costs.

However, the bank had concerns about customer adoption and surveyed their customer base to validate customers' readiness to accept mobile authentication. The data showed mixed results. Some clients were ready, others not. The bank determined that a hybrid implementation was the best strategy. In fact, their research confirmed that most customers actually want both.

Customers want the convenience of using their mobile device, knowing that if something goes wrong (e.g., lost phone, dead battery, etc.) they have a hardware backup.

While software authentication would provide cost savings, it was not without challenges. Some customers did not own a smartphone. Among those who did, survey results indicated resistance to change. While the mobile-first segment was interested in software authentication, not everyone wanted to use their smartphone as an authentication method.

In their communications, the bank had to overcome three barriers to adoption:

1. Lack of familiarity with, and trust in, mobile authentication.
2. Concerns about having too many apps already (not wanting to run out of space on the phone).
3. Concerns about loss or theft of the phone.

As a result, the bank decided to implement a hybrid hardware and software authentication system – while designing their customer communications to promote the software option.

> We noticed that initially, customers are resistant to change – but once they try mobile authentication, they are very satisfied and stay with it. That's why communication is so important. You have to convince customers to try it."
>
> **-Project Manager**

Requirements

To support the hybrid approach, the bank wanted a single vendor that could offer both authentication methods. That narrowed the shortlist to two vendors.

All other key requirements fell into three categories: security, client experience and pricing. For example:

Security expertise: The bank required a vendor and trusted partner with deep industry expertise. "The vendor was very aware of new regulations and was able to advise us on compliance," says the Project Manager.

Customer experience: The bank needed a vendor with a proven track record for enabling a frictionless, but highly secure, customer experience.

Local distribution center: The bank had a requirement for proven security practices around the physical distribution of new hardware devices, since the vendor would have to handle private customer data. The bank required that PII remain in-country. The vendor's distribution center was a differentiator.

Pricing: According to the Project Manager, "In terms of cost, the vendor was very close to the competing vendor."

The Solution

In addition to switching their hardware devices to OneSpan, the bank also integrated OneSpan software directly into their mobile and online applications.

Through the OneSpan Mobile Security Suite library of APIs, the bank added application security, authentication and dynamic signing features.

To implement the solution, the bank assembled a team composed primarily of internal resources. These included:

- members of the security department
- a core team of six part-time developers
- the bank's change management team

Rollout & Adoption

From 2016 to 2017, the bank prioritized deployment to two streams of customers: those whose hardware tokens were about to expire and mobile app users.

The bank communicated the change to customers via email notifications, the website (a dedicated page with information, videos and FAQs) and helpdesk.

To date, the bank has migrated 30 percent of their customers. Rather than take a big bang approach, the bank chose to deploy gradually for two reasons:

- **Helpdesk pressure:** Migrating everyone at the same time would have made it difficult to handle call volume, even with external support.
- **Budget:** The bank has many customers whose hardware device battery life is still valid. These customers can continue to use it until the enforcement of the new regulation in 2018.

From the Bank's Experience, Customer Adoption Depends on:

- How you communicate the value to clients
- What options you offer

The way the bank explains the new authentication methods to customers directly influences adoption. Today, the bank first promotes the software method. If the customer does not have a smartphone, then the bank will present the hardware option.

"If you ask them to choose between A and B, it is very likely the adoption [of software] will be lower because customers are not always ready to change. The reason adoption is so high, is because today, in our emails to customers, we only promote the soft key," says the Project Manager.

This was one of the learnings from the initial rollout in 2016, when the bank offered customers a choice of hardware or software authentication. The following year, the bank changed their approach. By only promoting mobile authentication, the banks saw a significant lift in activations, with 62 percent of customers activating the soft key.

Tips for a Successful Initialization

The solution provides a full range of processes for deployment, provisioning and activation of authentication solutions. These processes ensure secure generation, storage and delivery of personalized credentials to users, preventing credential theft attacks. In most implementations, banks are able to reuse existing practices and communication methods with their clients, to eliminate helpdesk overload and reduce security risks. This secures banks from fraudsters who tend to use switching periods to run social engineering attacks.

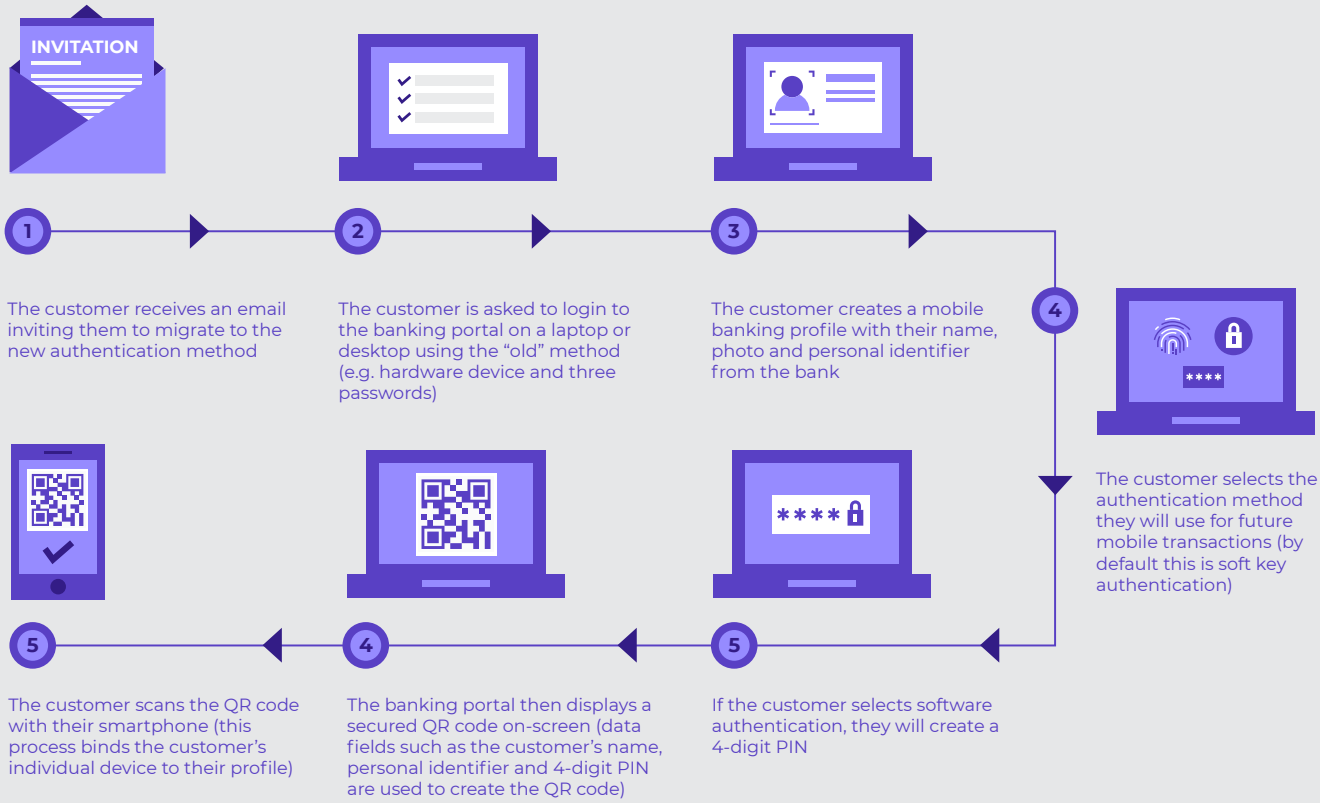
During the implementation phase of the project, OneSpan's UX and security consultants worked with bank personnel to develop credential management processes. For example:

OneSpan's solution offers multiple ways to activate the software token. This allows the bank to create user-friendly workflows for migration from old tokens to the new method.

- Digipass® for Apps provides unique secure visual technology known as Cronto, which allows users to activate their credentials in seconds.
- Because it is natively integrated inside the bank's mobile app, Digipass for Apps provides automatic linking of the customer's account with their security credentials and device-specific data.

WORKFLOW DIAGRAM

Prior to using OneSpan, the login page for the bank's mobile app mirrored the login for the banking portal. However, research showed that multiple family members had a tendency to use the same tablet. As a result, the bank introduced profiles on the app. Instead of re-entering login details each time, customers could now setup and store their profile on the app. The process of creating the profile and activating the software authentication took place simultaneously. Here's how:



The Benefits

One of the most noticeable benefits was the level of customer satisfaction among those who tried the soft key authentication. According to the Project Manager, "Feedback from people who have activated the soft key has been very positive. It's a lot easier to use. They always have it on them. It goes a lot faster because it uses a PIN rather than passwords that customers forget."

Project stakeholders were pleased with:

- The ease of integration into the banking app;
- The fact that the bank did not have to point customers to a separate app solely for authentication;
- The overall coverage of security threats in the OneSpan Mobile Security Suite, which provides customers with a trusted authentication solution through their favorite mobile devices;
- The quality of post-sale support they received from the OneSpan team.

Learnings

"Overall, the majority of customers did not have any trouble understanding mobile authentication, and were very happy we introduced it," says the Project Manager. "They found the information on the website, read it, and were able to activate and start using it without any helpdesk support."

However, one of the key learnings was the importance of adequately preparing for customers who will need support. A small percentage can generate a heavy workload for the helpdesk. "We were not fully ready for that. We had to scale up our helpdesk team very quickly," says the Project Manager.

A second lesson was the importance of tailoring the customer communications. Best practice is to segment and customize communications to different user groups since, "...not all customers are know what a QR code is. Not all are tech savvy – some do not trust new authentication methods. Taking the time to adjust the communications is very important. That will make it clearer and easier for all."

Finally, making educational and instructional videos was a big win for the bank. Not all customers will take the time to thoroughly read the information on the website – or the emails from the bank. "We were very happy we had those videos," says the Project Manager.

One of the additional advantages of using video is branding. Because OneSpan's technology is white labeled, this gives banks the opportunity to promote their own brand to their customers, reinforcing the bank's reputation as an innovator.

Conclusion

- Software authentication provides compelling benefits – greater security, a simpler user experience and significant cost savings. But as highlighted in this case study, a successful migration requires a balance of leading-edge technology and proven practices for managing change and driving adoption. Our experience with banks around the world has positioned OneSpan as a trusted partner for mobile authentication, both for our technology and our consultative approach. If you are considering migrating customers to mobile authentication, contact us to discuss your project.

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 fraud 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