# Case Study: NewB Bank

## EXECUTIVE SUMMARY

### Business Objectives

As a new digital-only bank, it was critical that NewB implement the right security to build trust and protect their brand.

### The Challenge

NewB needed proven authentication and mobile security solutions implemented in a tight timeframe. With their banking license at stake, delays were not an option.

### The Solution

- OneSpan Cloud Authentication
- OneSpan Mobile Security Suite
- OneSpan Mobile App Shielding

### Results

- Strong protection against social engineering, banking Trojans, mobile malware and other attacks
- Implemented ahead of deadline
- Live in 4 months with the authentication solution
- Mobile app shielding configured and deployed in days
- Facilitated compliance with PSD2
- Cost effective and user friendly
- Agility and speed of cloud infrastructure

NewB is the first new bank in Belgium in 40 years. As a digital bank, it serves customers exclusively through its online portal and mobile app. What differentiates NewB is its vision. It is an ethical, co-operative bank that serves society by investing in projects that respect the planet and human rights. As a co-op, every member has a voice regardless of the size of their investment in the bank; the members are the owners and they decide how their money will be managed within the bank.

While NewB is a newcomer to the banking sector, their success story has been seven years in the making. NewB overcame multiple challenges along the way and after years of hard work, officially began operating as a licensed bank in 2020.

## The Race for a Banking License

While NewB first started as a social movement in Belgium in 2013, it wasn't until 2016 that it launched its first offering, the Goodpay prepaid card. By 2018, NewB had introduced insurance products to the market. From there, the co-op began laying the groundwork to obtain a banking license.

In October 2019, the Financial Services and Markets Authority approved NewB's prospectus and NewB began raising funds.[1] This marked a critical milestone for NewB. They had to raise €30 million by the end of the following month. If NewB did not succeed in attaining

this target, the European Central Bank would not approve a banking license.

With the help of more than 70,000 investors — from private individuals to government agencies and companies — NewB raised a total of €35 million. The co-op obtained its banking license in January 2020 and began formally onboarding members. Ten months later in November 2020, the first account holders were able to have their pay deposited into their NewB account.

Today, the bank offers personal accounts, personal loans, and all standard payment services. With consumers using NewB's digital apps, it was essential that the bank implement the right security to protect members against social engineering, mobile malware and other types of fraud attacks.

## Onto the Next Challenge: Finding the Right Digital Security Provider

Obtaining a banking license prompted a critical next step: evaluating security vendors for strong customer authentication, dynamic linking, mobile application shielding, and device binding solutions.

"We had to make a decision about which partner to work with and then we had to implement very quickly," says Adrien Liénard, Project Manager, NewB. "While we initially had contact with security vendors in 2019, at that moment we didn't have a banking license. We had to wait until the banking license was issued before signing an agreement and beginning implementation."

The first step was to identify the right security technology provider. NewB needed a strong partner with extensive banking industry experience, a proven security solution portfolio, and a track record for successful implementations.

## PSD2 Compliant, with a Strong Defense Against Fraud

The need to authenticate financial transactions using dynamic linking is one of the key requirements of PSD2.

Legislators introduced this requirement to prevent cybercriminals from altering transactions after the payer authenticates it. Such an attack could change a genuine transfer of 100 Euro to a friend, into a rogue transfer of 1000 Euro to an imposter.

PSD2 specifies that in the case of a payment transaction, the authentication code must be dynamically linked to two data points: the value of the transaction and the payee. If either changes during the transaction, the authentication code must also change. Further, payment information needs to be exchanged through a secure channel and it must be clearly shown to the user.

OneSpan's Cronto technology enables banks to comply with these requirements in a way that's quick and easy for users.

With NewB's banking license at stake, they could not compromise on security or timeline. OneSpan met this challenge with high-quality security, deployed ahead of schedule.

In addition, NewB could not risk any delays because their banking license was at stake. "In Belgium, according to the law, when you get a banking license you have one year to start your banking activities. That meant we had to be live with our banking activities by the end of January 2021," Adrien Liénard explains.

It was critical that everything happen quickly and on time. There could not be any delays that would impact the ability to launch the new bank. Further, NewB's leadership had announced during the fundraising campaign that they would launch the bank in 2020. Meeting the deadline was not only a question of legal compliance, but also public trust.

After an evaluation of leading security vendors, NewB selected OneSpan for the authentication solution.

"A partner's expertise and reputation is just as important as the capabilities of the solution itself," says Adrien Liénard. "The authorities are going to scrutinize new banks, it's part of being new to the market. We know they are looking at NewB and it reassures them to see us working with trusted partners. OneSpan works with most of the banks in Belgium and that gave us credibility in the eyes of the National Bank."

NewB also selected MAINSYS as the integration partner for this project. MAINSYS provides NewB's core banking system and is a Belgian IT services and software company specialized in the financial sector.

## Cloud-based Authentication: Speed and Agility

The first solution NewB implemented is OneSpan Cloud Authentication (OCA). OneSpan Cloud Authentication offers extensive authentication options. This provides the security NewB needs to protect its members from fraud attacks, with the modern experience that members expect of a digital-only bank.

When designing their authentication experience, NewB selected two authentication methods: the software Cronto® transaction signing solution and its hardware equivalent, the Digipass® 772 hardware authenticators.

## Cronto Technology Provides the Best of Both Worlds

As a new startup, NewB is very cost-conscious and had to carefully consider what authentication methods they would select.

In Belgium, most banks rely on bank card readers. The bank evaluated this option, but in NewB's case this type of authentication device came with drawbacks. Considering that NewB was not planning to issue a debit card until June 2021, selecting the card reader option would have meant that their members could not start transacting right away in January 2021 when the bank opened for business.

NewB also wanted to avoid the expense of sending hardware devices to every member.

"OneSpan's reputation in the market, security expertise, and experience with PSD2 have made a real difference for us. For example, recently we had to send a PSD2 report to the National Bank. We asked OneSpan for help and in 24 hours we had the answers. That was a value-add for us, to know OneSpan has our back."

**ADRIEN LIÉNARD**
PROJECT MANAGER, NEWB

That's when the bank learned of OneSpan's **Cronto** technology. Cronto is an out-of-band authentication technology that helps financial institutions drive down fraud. It reduces the risk of social engineering, where customers can be tricked into revealing an authentication code — and also protects against banking Trojans, a technique that criminals use to intercept banking credentials and manipulate financial transactions.

Cronto displays a QR-like code onscreen that people scan with either their phone or hardware authenticator to authenticate quickly and securely. Unlike card readers, Cronto functionality is available in both software and hardware. This gives members options in how they prefer to authenticate, while maintaining the same user experience and security across the entire customer base.

It was especially interesting for NewB because many — but not all — of their members are mobile users and having a software authentication option would eliminate the need to send card readers by mail or courier to the majority of their customer base.

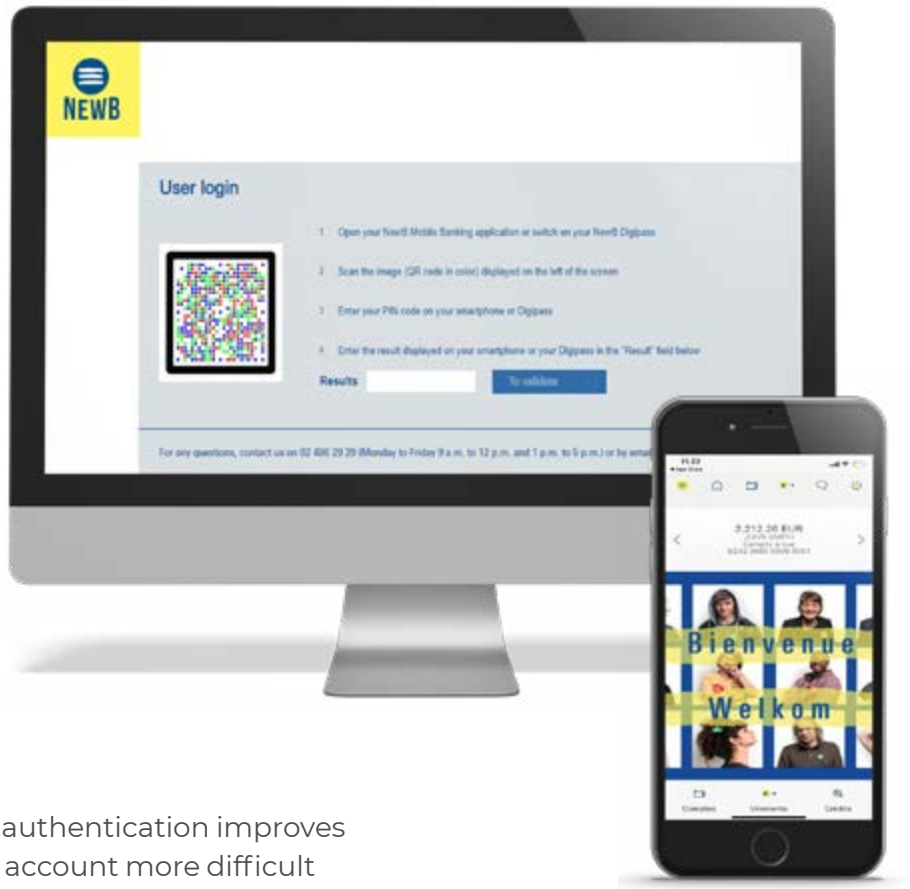
"That cost savings was a big advantage for us," explains Liénard.

In addition, OneSpan's Cronto technology removed the administrative workload that comes with issuing card readers to members who don't have a smartphone. The Digipass 772 is a non-personalized device, so it doesn't need to be manually assigned to a member beforehand like a card reader does. This made it easier for NewB to manage because they can bulk-send Digipass devices, and each member activates it themselves online via a self-serve portal. The activation process links the hardware device to the individual's user profile.

"The main reason why we chose Cronto was because of user friendliness and having the same user experience for everyone. The deciding factors were cost, user friendliness, and the fact that it would allow us to launch the bank before our debit cards were available."

## The User Experience

At NewB, the two authentication use cases are secure login and transaction signing.




**THIS IS HOW IT WORKS:**

**Members who have a smartphone:** For online banking: Members can use their mobile phone to scan a Cronto code displayed on the online banking portal. This generates a one-time passcode (OTP) on the smartphone. The member then enters the OTP into their online banking session and they are successfully logged in or the transaction is authorized.

Because the security code is generated in a different channel independent of the online banking session, it is considered out-of-band. Out-of-band authentication improves security because it makes breaching an account more difficult due to two separate and unconnected authentication channels that would need to be simultaneously compromised for an attacker to gain access.

**For mobile banking:** In the NewB mobile app, members enter a PIN or biometric factor (e.g., facial scan, fingerprint) to login to the app or authorize a transaction in the app.

**MEMBERS WHO DO NOT HAVE A SMARTPHONE:**

If a member does not have a smartphone, they will use a Digipass 772 hardware device to scan the QR-like code.

## Deployed Ahead of Schedule

"We started the integration in July. The goal was to be live by early November 2020, because that's when we would be connected to the payments system in Europe. It was critical that we would be connected by then," says Adrien Liénard.

All of the integration for the online banking channel was completed in four months. The first technical meeting between

NewB, MAINSYS and OneSpan was held in March 2020. That summer, the OneSpan solution was implemented and NewB's online banking was connected.

"The time constraints were tight, so we prioritized the implemention of OneSpan's Cronto technology and Digipass authenticators for online banking. Once that was completed, we began phase two which was the mobile development," explains Mathieu Latour, Project Manager at MAINSYS.

"It was very important to NewB that members without a cell phone could securely authenticate just as easily as those with a mobile. OneSpan solves this by offering their solution in both a software and hardware format, which provides the same user experience and authentication flows to all users. That made the difference — and helped shorten the implementation timeline."

## The Mobile App Shielding Component of NewB's Solution

The second component of NewB's solution is the OneSpan Mobile Security Suite (MSS), which enables mobile developers to integrate additional security features with their app. Of these mobile security features, NewB selected the **mobile application shielding** capability.

"We needed only a few days to configure the OneSpan mobile app shielding capability to protect the NewB mobile banking app we had just developed," says Mathieu Latour.

Mobile app shielding is a low-code technology that safeguards against the latest mobile banking Trojans, reverse-engineering techniques, several types of runtime threats, and methods that attackers use to steal banking credentials and hijack banking transactions. It also creates a secure execution environment, allowing mobile apps to operate safely even on untrusted mobile devices such as those that have been jailbroken.

PSD2 compliance was one of the reasons that led the bank to implement mobile app shielding. Known as "replication protection", this PSD2 requirement states that if a bank chooses to use a mobile app as a part of their authentication flows, they must take action to mitigate the risk of an attacker reverse-engineering the app to uncover and potentially reproduce the token secret used to generate an authentication code. Therefore, to comply with PSD2, banks need to protect the app against cloning. And as an added benefit of app shielding, the app is also protected against repackaging attacks.

Application shielding does this through a combination of preventive, detective, and reactive approaches. Code obfuscation is one example. To mitigate the risk of attackers reverse-engineering the app, code obfuscation increases the time and effort necessary to reverse engineer it. Runtime protection is another example. App shielding detects attacks at runtime, such as attempts to tamper with the app or run the app inside an emulator.

## Conclusion

As a neobank, NewB's strategy has been to work with established partners to build trust in their digital services, apps and brand.

"OneSpan's reputation in the market, security expertise, and experience with PSD2 have made a real difference for us," says Adrien Liénard. Not only in terms of the robust authentication technology, rapid implementation and smooth user experience, but also in facilitating compliance. "For example, recently we had to send a PSD2 report to the National Bank. We asked OneSpan for help and in 24 hours we had the answers. That was a value-add for us, to know OneSpan has our back."

At OneSpan, we understand the challenges of protecting the digital customer journey. In addition to proven technologies, we bring a highly consultative approach, deep regulatory expertise, and user experience best practices. To learn more about how OneSpan can help protect your customers from digital fraud, visit **OneSpan.com** or contact us.

**ENDNOTES**

1 https://mailchi.mp/newb/avag2019presse-355136?e=%5bUNIQID%5d

## About OneSpan

OneSpan helps protect the world from digital fraud by establishing trust in people's identities, the devices they use and the transactions they execute. We make digital banking accessible, secure, easy and valuable. OneSpan's Trusted Identity platform and security solutions significantly reduce digital transaction fraud and enable regulatory compliance for more than half of the top 100 global banks and thousands of financial institutions around the world. Whether automating agreements with identity verification and e-signatures, reducing fraud using advanced analytics, or transparently securing financial transactions, OneSpan helps lower costs and accelerate customer acquisition while improving the user experience.
Learn more at **OneSpan.com**.

**SOCIAL MEDIA**

**CONTACT US**
**OneSpan.com/contact-us**



CCST-NEWB-BANK-02112022