OneSpan

CASE STUDY

Raiffeisen

TRANSFORMING CUSTOMER EXPERIENCE THROUGH SECURITY

EXECUTIVE SUMMARY

Business Objectives

- Comply with PSD2 Strong Customer Authentication requirements, including Dynamic Linking and Replication Protection
- Provide an easier authentication experience for customers

Benefits

- Raiffeisen Italy is prepared for PSD2, well ahead of the September 2019 deadline
- The bank has both a secure system and a very simple customer experience
- High adoption and activation by customers
- Perceived by customers as innovative

Raiffeisen Italy Implements Mobile Authentication & Mobile App Shielding for PSD2 Compliance and Ease of Use

Raiffeisen Italy is the umbrella organization for 40 entities of Raiffeisen Bank in the Italian province of South Tyrol. Overseeing IT services for these member banks, Raiffeisen Information System CIO Alexander Kiesswetter modernized Raiffeisen Italy's authentication system to comply with the revised Payment Services Directive (PSD2). As part of that, Raiffeisen Italy introduced a mobile app that authenticates and secures users – built using the OneSpan Mobile Security Suite and white-labeled with the Raiffesien brand.

"In Italy, close to 50% of our customers are using internet banking and 20% are using mobile. But we are seeing a much faster increase in the adoption of mobile banking compared to internet banking," Alexander Kiesswetter says.

While PSD2 was the main driver, the rapid shift to digital and mobile banking made it equally important for Raiffeisen Italy to offer both strong security and an easier user experience. Simply put, customers no longer want to pull out their bank card and hardware token for every small transaction – preferring instead to authenticate through their mobile device.

"Mobile-first is an important part of our digital transformation strategy. That's why OneSpan was perfect for us. For the first time, we have a solution that enables us to move services completely to the smartphone without using other hardware tools for the authentication. Now, we can use not only the PIN for the authentication, but also Face ID and Touch ID."

"We selected OneSpan's innovative solutions because they provide a high level of security and usability. Traditionally, it's very difficult to combine the two – until now, it's always been a trade-off. We wanted to innovate and simplify the customer experience. With OneSpan, we were able to do that."

Alexander Kiesswetter
Raiffeisen Information System CIO

SHARE THIS

The Challenge

As the CIO, Alexander Kiesswetter faced two challenges: PSD2 compliance and a legacy authentication system that customers found difficult to use.

PSD2 compliance is a key priority for financial institutions (FIs) across Europe. FIs need to comply with the requirements for Strong Customer Authentication and Transaction Risk Analysis. In addition, Raiffeisen Italy had to meet two other requirements:

- **Dynamic Linking:** For remote payment transactions, PSD2 requires that FIs apply authentication that dynamically links the transaction to a specific amount and payee. Throughout the authentication process, the confidentiality, integrity, and authenticity of payment information needs to be protected, and the user must be made aware of the amount and the payee.
- **Replication Protection:** 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, FIs have to protect the possession element (in this case, the app) against cloning.

Further, the bank wanted to provide an easier authentication experience for customers. The problem was, they found themselves in the conventional tug-of-war between security and ease of use – with security winning at the expense of customer experience. While their legacy authentication system was very secure, customers complained it was burdensome.

"Until we started using OneSpan, our attention was focused on security. That's why we used separate hardware tokens with bank cards, because we weren't convinced that an alternative would give us enough security," says Kiesswetter.

Evaluation and Selection

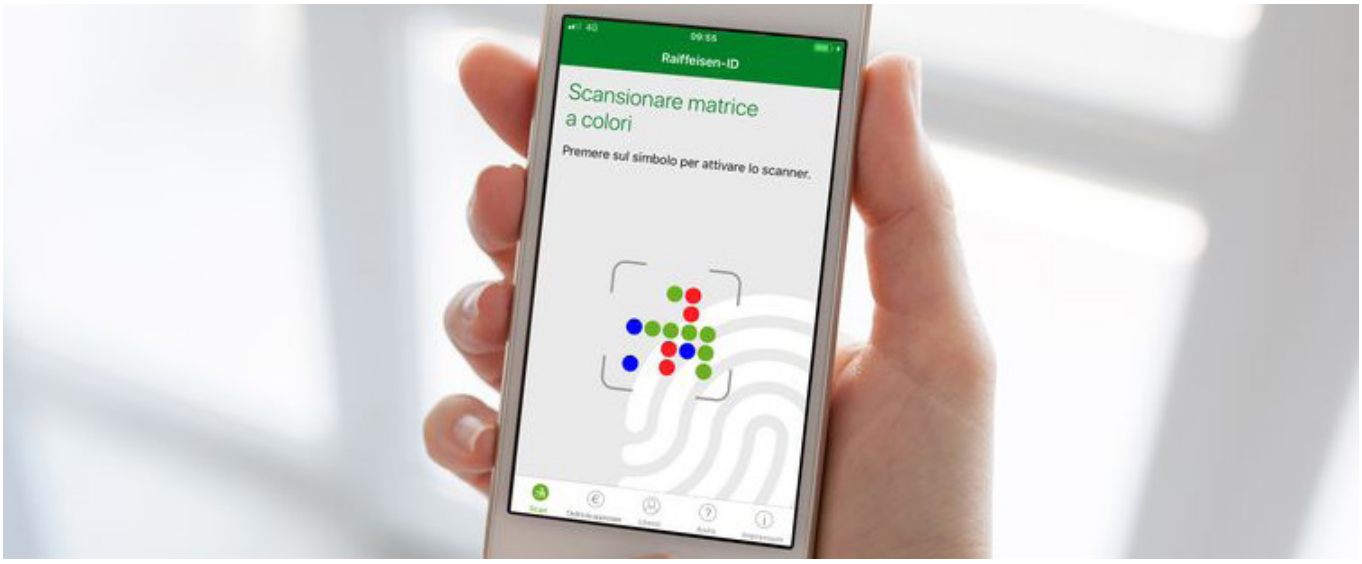
For Raiffeisen Italy, choosing best-of-breed technologies through the right network of IT security partners, is core to their success. An in-house build was never an option, so the CIO tasked two teams with evaluating solutions:

- For authentication, a group of IT technicians made the software selection.
- For mobile app security, the evaluation team included the CISO, an IT Architect, and representatives from the risk and compliance, software development, and customer support teams.

"During the selection process, we evaluated several companies. The big difference we saw between OneSpan and other vendors was OneSpan's solutions combine a high level of security and compliance with a high level of usability."

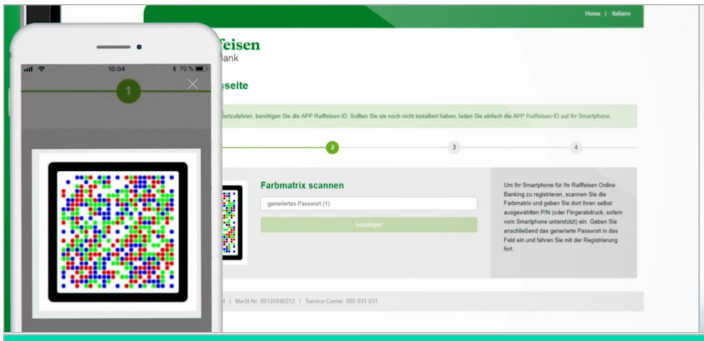
As part of the evaluation process, Raiffeisen turned to other banks in their network, primarily in Germany and Austria, to learn from peers. Finally, the bank also ran internal tests to evaluate the technology and user experience. They did a customer survey, in-house workshops, and a proof-of-concept (POC).

"What we found was that with customers, there was great acceptance and willingness to use a smartphone-based solution," says the CIO.

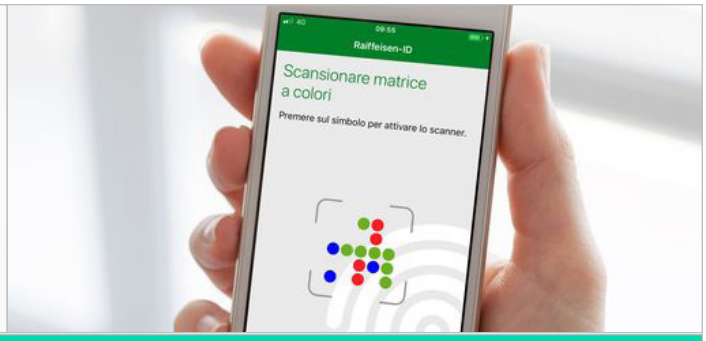


Key Requirements & Evaluation Criteria

Dynamic Linking



Replication Protection



OBJECTIVE	
Protect customers' online and mobile banking transactions against fraud, including banking Trojans and social engineering attacks such as phishing and man-in-the-browser attacks.	Protect Raiffeisen's authentication app against intrusion, tampering, and reverse engineering.
ONESPAN TECHNOLOGY EVALUATED	
OneSpan's Cronto® technology is based on color cryptograms that can only be read by a trusted device. Cronto uses a unique visual challenge contained in a graphical cryptogram consisting of a matrix of colored dots displayed on the customer's PC screen. The customer uses the camera in their mobile phone to capture this cryptogram by scanning the screen, instantly decoding, decrypting and displaying transaction details for user verification. If the image has not been tampered with, the customer is then presented with transaction information, like payment details, decoded securely from the visual cryptogram image.	The OneSpan Mobile Security Suite enables mobile developers to natively integrate security features such as two-factor authentication, geolocation, jailbreak and root detection, device ID, and other security features into an app. One of 17 SDKs in the Suite, app shielding detects and interrupts potential mobile attacks in real-time. In order to create a secure execution environment for mobile apps, they should be protected using application shielding with runtime protection. This technology protects a mobile app against several types of runtime threats. It creates a secure execution environment for mobile apps, allowing them to be executed even on untrustworthy mobile devices. Application shielding uses a combination of preventive, detective, and reactive approaches. It mitigates runtime threats, for instance, by obfuscating code to make reverse engineering more difficult. It detects attacks at runtime, such as attempts to tamper with the app or run the app inside an emulator. Finally, it can react to runtime attacks in different ways, such as alerting the bank's server-side risk engines, or even shutting down the app.
KEY EVALUATION CRITERIA	
• An easy enrolment and signature process that enables the bank to meet PSD2 requirements with minimal impact on the user experience. • Support for FaceID or TouchID, in addition to a PIN for the authentication. • Use of encrypted out-of-band communication. • Push notification: For mobile transactions, the ability to transfer the transaction data from the banking server to the mobile banking app using an encrypted push notification message.	• Invisible security: Runtime protection provides continuous monitoring and defense, without interrupting the customer experience. • Easy integration that does not place a burden on developers. • Dynamic protection that detects and mitigates runtime attacks on a mobile app so the app can run securely even in hostile or compromised environments.

A Dual Solution

Using the OneSpan Mobile Security Suite library of APIs, Raiffeisen Italy added transaction signing to secure customers' online transactions against fraud. They also integrated mobile app shielding to protect their mobile authenticator app. This solution enabled the bank to comply with the PSD2 requirements for:

- **Dynamic Linking:** The bank implemented Cronto technology, which uses a graphical cryptogram made of colored dots to encrypt transaction details. Used by banks throughout Europe and around the world, Cronto meets the PSD2 authentication and dynamic linking requirements for securing financial transactions with minimal impact to the user experience.
- **Replication Protection:** As part of its mobile-first strategy, Raiffeisen Italy launched a mobile banking application that authenticates and secures users. The bank took a leadership role as first-to-market in Italy to protect its app with mobile app shielding.

The innovative aspect of OneSpan's mobile app shielding with runtime protection was one of the reasons that led the bank to choose this technology.

"It's the first time that we use a system that is based on the smartphone, because until this product, we were convinced that the smartphone is by definition an insecure device. When we saw the way that OneSpan enforces the security on the smartphone, and also the continuous updates to the software of the smartphone, we were convinced that finally, here was a product that we can offer to our customers and that guarantees us a high level of security."

The Benefits

Raiffeisen Itay has received positive customer feedback and experienced high adoption of the new authentication app.

"Customers perceive Raiffeisen once again as an innovative bank," says the CIO. "The feedback that reached me is that customers are very satisfied by the new functionality. We also ran a marketing launch for the new authentication app. During the marketing launch, we saw that the marketing effort created a lot of expectation among customers. When we launched it, there was much demand and high activation, all positive signals from the market that they accepted it very well."

In addition, Raiffeisen Italy is prepared for PSD2, well ahead of the September 2019 deadline. Kiesswetter explained that, "Regarding the PSD2 requirements, we are ahead in the market."

Conclusion

"From working on this project, my advice to other banks is to start their digital transformation on the front lines, at the touchpoint with the customer. That is where the innovation is most important. Choose a strong partner with a strategic view of where your digital transformation can go in the future. Start on the front lines, work on the customer touchpoints, and choose a partner who has clear vision about where digital transformation will go in the next few years."

"Partner vision is important. Having worked with OneSpan, we see things differently. This project changed our mindset. Instead of having to choose between security and customer experience, it really can be both. I think that's the biggest surprise. Moving forward now, we will continue to innovate and work on our system knowing we can have a secure system, as well as a very simple and positive customer experience. So, that principle will now guide our vision for the future."

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

Copyright © 2018 OneSpan North America Inc., all rights reserved. OneSpan™, DIGIPASS® and CRONTO® are registered or unregistered trademarks of OneSpan North America Inc. and/or OneSpan International GmbH in the U.S. and other countries. All other trademarks or trade names are the property of their respective owners. OneSpan reserves the right to make changes to specifications at any time and without notice. The information furnished by OneSpan in this document is believed to be accurate and reliable. However, OneSpan may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.
Last Update October 2018.