



Case study

Ensuring the protection of users' most valuable online information

Leading digital identity app leverages OneSpan for end-to-end mobile app security



Industry
Financial services
Software



Region
Europe



Insight
Leading provider of
ID wallet solutions

Introduction

To safeguard the personal information and authentication credentials of its users while ensuring compliance with the stringent eIDAS 2.0 regulatory frameworks mandated by the European Union (EU), the company embarked on a search for a security partner. Following an exhaustive assessment of the leading vendors in the mobile app security market, the company selected OneSpan to secure its digital ID app.

About our client

Our client is one of Europe’s leading digital identity application providers, enabling millions of users to securely manage, verify, and access highly sensitive personal and digital information online. Operating at the core of the digital trust ecosystem, the platform plays a critical role in enabling secure authentication and identity verification across a wide range of services and use cases.

As a key player in the European digital identity landscape, the organization operates in a highly regulated environment where security, privacy, and compliance are essential. It must meet stringent regulatory standards while defending against an evolving threat landscape targeting mobile applications and identity infrastructure. At the same time, it is committed to delivering a seamless user experience while scaling securely across a rapidly growing user base in Europe.

Challenge

As digital identity becomes increasingly central to secure access across Europe, the threat landscape targeting mobile applications has grown more sophisticated and persistent. In this context, the organization needed to strengthen its mobile security posture across both application and backend layers, ensuring robust protection of sensitive data while maintaining a seamless user experience and meeting strict regulatory requirements.



Protecting sensitive data and cryptographic assets

A key challenge was securing sensitive user data and cryptographic keys within the mobile application. With mobile environments increasingly targeted by attackers, risks such as reverse engineering, code tampering, and credential extraction had to be effectively mitigated to maintain trust in the platform.



Securing infrastructure and ensuring regulatory compliance

The organization also needed to address vulnerabilities in backend communications and server-side infrastructure. This required a broader security approach beyond the mobile app while ensuring full compliance with strict European regulations, including eIDAS 2.0, without impacting performance or user experience.



Solution

Timely and successful eIDAS 2.0 certification. Following the deployment of OneSpan, the company obtained eIDAS 2.0 certification from the German National Cyber Security Authority. The app successfully passed mobile app penetration tests required by the Federal Office for Information Security (BSI), thereby meeting the rigorous standards set by the EU for online identity platforms.

Business benefits

The implementation of advanced mobile app security delivered measurable advantages across user experience, security resilience, and development flexibility:

- Simplified online activities via optimized security and safely storing users' personal information and credentials.
- Effective mobile app self-protection thwarts attempts to extract precious cryptographic keys.
- Developers have full control over security library integration in the ID app, enabling deeper customization and enhanced security.
- Coverage for 99% of smartphones in use worldwide, spanning various operating systems and manufacturers.



Securing everyday online activities with the company's ID app

The company provides a secure digital ID solution with an app that simplifies online activities by safely storing users' personal information and credentials.



All-in-one digital identity solution

The ID solution serves as an all-in-one digital identity solution. It eliminates the need for multiple usernames and passwords, acting like a digital passport on users' mobile devices or computers. Beyond identification, it enables users to authenticate themselves, access services, sign documents, and make payments. For instance, when opening an online bank account, the ID solution streamlines the process by verifying identity and transferring required data without manual form filling.



Secure data storage and sharing

The ID solution securely stores users' identity data in one location, facilitating easy sharing with online service providers. Users retain complete control over the information shared with each provider.



Simplified login

With the ID solution, users only need one login method for multiple services. Rather than managing numerous passwords, they can link their account to partner companies, granting access to all associated accounts using the ID solution.



Effortless electronic signatures

The ID solution allows for electronic signatures, ensuring the authenticity of the signer. Whether on the company's platform or integrated with third-party electronic signature services, the company offers qualified electronic signatures (QES) as per eIDAS 2.0 regulations.



Streamlined payments

The solution simplifies online shopping. Users enter their banking details once in their account, expediting the purchase process. Logging in with the ID solution automatically shares payment information, eliminating the need for manual data entry.



Cryptographic keys: Addressing the solution's prime vulnerability

Cryptographic keys in a mobile ID app are a major security vulnerability because they are central to securing the app and its data. These keys are vital for encrypting and decrypting sensitive information, such as user credentials and personal data. Compromised keys make it easy for attackers to decrypt and access protected data. They are also essential for secure communication with backend APIs, and if breached, attackers can intercept and manipulate data exchanges, posing a significant risk of unauthorized access and data breaches.



How hackers attempt to extract sensitive cryptographic keys

Hackers employ various techniques to extract these keys, including reverse engineering, exploiting mobile device vulnerabilities, and advanced methods like side channel attacks.

Reverse engineering

Hackers may use reverse engineering techniques to analyze the app's code and memory, seeking out cryptographic keys.

Mobile device vulnerabilities

Mobile devices can contain vulnerabilities that expose cryptographic keys stored within apps. For example, rooted or jailbroken devices are more vulnerable to attacks, making it easier to bypass protections and compromise sensitive data, including keys.

Side channel attacks

Side channel attacks employed by hackers exploit unintended information leakage during mobile app operation. Instead of attacking the app's code directly, these attacks analyze patterns like power consumption, electromagnetic emissions, or timing variations generated by the app's execution. By deciphering these subtle signals, hackers can deduce sensitive information like cryptographic keys or user inputs without needing access to the app's source code. The subtlety and sophistication of side-channel attacks make them a potent threat to all mobile ID apps.

Ensuring top-tier mobile app security with OneSpan

To safeguard the personal information and authentication credentials of its users while ensuring compliance with the stringent eIDAS 2.0 regulatory frameworks mandated by the EU, the company embarked on a search for a security partner. Following an exhaustive assessment of the leading vendors in the mobile app security market, the company selected OneSpan to secure its digital ID app.



“Working with OneSpan has been instrumental in strengthening our digital identity security and meeting strict eIDAS and German regulatory standards.”

Chief Information Security Officer
Leading Provider of ID Wallet Solutions



Superior mobile app self-protection as the decisive factor in choosing OneSpan

The company recognized that OneSpan would effectively thwart attempts to extract its app's precious cryptographic keys when attackers attempt to reverse engineer the code, inject malicious code at runtime, exploit vulnerabilities on jailbroken (iOS) or rooted (Android) devices, or employ more sophisticated methods like side channel attacks.

The digital ID app also acknowledged that, unlike less sophisticated post-coding alternatives, OneSpan grants developers comprehensive control over the integration of security libraries within the ID app. This allows for a deeper level of customization and enhanced security.

Thwarting side-channel attacks with strong cryptography

The company recognized that OneSpan's state-of-the-art cryptographic features offered unparalleled protection against advanced threats targeting its cryptographic keys, including side channel attacks. OneSpan employs robust cryptography tailored to each device and operating system, thereby delivering optimal protection across all devices, and ensuring exceptional 100% coverage.



Protection from server-side vulnerabilities

The company's server-side APIs were vulnerable to security attacks. OneSpan's server-side active hardening capabilities enhance app-level security by verifying device binding information and equipping each app instance with unique cryptographic keys and certificates. This not only strengthens the app itself but also reinforces the overall security of the entire mobile technology stack, including its backend APIs. In practice, only app instances with legitimate and valid encryption-based individualization are granted permission to interact with backend APIs, effectively preventing API abuse and API scraping attacks.



OneSpan: Your partner for timely and successful eIDAS 2.0 certification

OneSpan's support for over 99% of smartphones in use worldwide, across a wide range of operating systems, device models, and manufacturers, was also a key factor in the company's decision, ensuring broad compatibility, seamless deployment, and consistent security coverage for its entire user base.



Successful eIDAS 2.0 certification

Following the deployment of OneSpan, the company successfully obtained eIDAS 2.0 certification from the German National Cyber Security Authority. The app also passed comprehensive mobile app penetration tests required by the Federal Office for Information Security (BSI), demonstrating compliance with the rigorous security, identity, and trust standards established by the European Union for online identity platforms.

“Collaborating closely with the foremost European ID Wallet provider has been a transformative journey for us at OneSpan. By investing in stringent regulatory compliance, meeting the rigorous standards of eIDAS, and earning evaluations from the German Ministry of the Interior (BMI) and the Federal Information Security Agency (BSI), we've not only fortified our position but set the gold standard in ID Wallet security. The company's technology, seamlessly integrated into Deutsche Bank and entrusted with the ID management of 9 million Barmer policyholders in Germany, underscores the value of prioritizing security and regulatory adherence in the digital identity landscape. This case study is a testament to the dividends reaped when excellence meets innovation in robust and secure digital identity solutions.”

Pedro Hernandez
Senior Director, Business Development & Strategic Partnerships, OneSpan

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
OneSpan.com/security

Contact us at
OneSpan.com/contact-us



Copyright© 2026 OneSpan North America Inc., all rights reserved. OneSpan®, the “O” logo, DigipassONE®, Crono® are registered or unregistered trademarks of OneSpan North America Inc. or its affiliates in the U.S. and other countries. Any other trademarks cited herein are the property of their respective owners. This content is provided for informational purposes only and is provided “as is,” without warranty of any kind, whether express, implied, statutory, or otherwise, including without limitation warranties of merchantability, fitness for a particular purpose, or non-infringement. Product specifications, features, roadmaps, and availability are subject to change without notice and do not represent a commitment. OneSpan does not warrant that any specifications or performance characteristics described herein will be achieved in all operating environments. Last updated: July 2026.