CASE STUDY

>Protecting users' most valuable online information_

Digital identity app partners with Build38 to ensure end-to-end mobile app security

Summary

A leading digital identity app company needed to safeguard the personal information and authentication credentials of its users, and ensure compliance with the stringent eIDAS 2 regulatory frameworks mandated by the European Union (EU).

It embarked on a search for a security partner that would help it achieve its goals. After an exhaustive assessment of the leading vendors in the mobile app security market, the company chose Build38 to secure its digital ID app.

Industry

Software Development
ID Management
Financial Services

Region

Europe

Insights

Leading provider of identity credentials

Key challenges

- Complying with EU's eIDAS 2 regulations—crucial for protecting user data and ensuring compliance
- Addressing security concerns and potential threats, including cryptographic vulnerabilities, server-side API attacks, side-channel attacks
- Ensuring broad device compatibility

The solution

Timely and successful eIDAS 2 certification.
Once Build38 was deployed, the company obtained eIDAS 2 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 European Union (EU) for online identity platforms.

Business benefits

- Online activities are simplified, thanks to optimized security
- Users' personal information and credentials are stored safely
- Effective mobile app self-protection thwarts attempts to extract precious cryptographic keys
- Developers have full control over security library integration in the ID app, allowing for deeper customization and enhanced security
- Coverage for 99% of smartphones in use worldwide, spanning various operating systems and manufacturers

The technology: Simplifying everyday online activities with a secure ID app

The company's secure digital ID app simplifies online activities like shopping, accessing services, and electronic signature, by safely storing and certifying its users' personal information and credentials.

An all-in-one digital identity solution

The all-in-one digital identity solution eliminates the need for multiple usernames and passwords, acting like a digital passport on users' mobile devices or computers. Beyond identification, it allows users to authenticate themselves, access services, sign documents, and make payments. For example, 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 app 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 app, 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 via the ID solution.

Effortless electronic signatures

Whether it's on the solution's own application platform or integrated with third-party electronic signature services, the company's technology provides Qualified Electronic Signatures (QES) that certify the signatory's authenticity and conform to eIDAS 2 regulations.

Streamlined payments

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

Cryptographic keys: A prime vulnerability

Cryptographic keys are a major security vulnerability in mobile ID solutions because they play a central role in securing both the app and its data. Since they are used to encrypt and decrypt sensitive information like user credentials or personal details, compromised keys make it easy for attackers to decrypt and access the same protected data. Cryptographic keys are also used to secure communications with back-end APIs, so if breached, attackers can intercept and manipulate data exchanges, opening the door to unauthorized access and data breaches.

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 themselves may possess vulnerabilities that can be exploited to jeopardize the security of cryptographic keys stored within apps. For instance, when a device is rooted or jailbroken, it becomes more accessible for attackers to breach sensitive data, including keys.

Side channel attacks

Side channel attacks, employed by hackers, exploit information that is unintentionally leaked when a mobile app is in use. Instead of attacking the app code directly, these attacks analyze patterns in power consumption, electromagnetic emissions, or timing variations generated when it executes. By deciphering these subtle signals, hackers can deduce sensitive information like cryptographic keys or user inputs without needing access to the app source code. The subtlety and sophistication of side-channel attacks make them a significant threat to all mobile ID apps.

Ensuring top-tier mobile app security with Build38

On a mission to safeguard the personal information and authentication credentials of its users while ensuring compliance with the stringent eIDAS 2 regulatory frameworks mandated by the European Union (EU), the company embarked on a search for a security partner. After an exhaustive assessment of the leading vendors in the mobile app security market, they selected Build38 to secure their digital ID app.

Superior mobile app self-protection

Build38s unmatched mobile app self-protection capabilities made it the clear choice

The company recognized that Build38 would effectively thwart attempts to extract its app's precious cryptographic keys and keep hackers from reverse engineering their code; injecting malicious code at runtime; exploiting vulnerabilities on jailbroken (iOS) or rooted (Android) devices; or employing sophisticated methods like side channel attacks.

The digital ID company also appreciated that, unlike less sophisticated post-coding alternatives, Build38 offered developers full control over how their security libraries were integrated into its ID app, allowing for a deeper level of customization and enhanced security.

Thwarting side-channel attacks with strong cryptography

The company recognized that the Build38's platform's state-of-the-art cryptographic features offered unparalleled protection against advanced threats targeting its cryptographic keys, including side channel attacks. Build38 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 are vulnerable to security attacks. Build38's server-side active app 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.

Support for 99% of smartphones worldwide

Build38 supports over 99% of smartphones in use worldwide, spanning a wide range of operating systems and manufacturers. This played a crucial factor in the company's decision to partner with them.

Achieving secure eIDAS 2 certification with Build38

With Build38 as their security partner, the company successfully met stringent EU standards

Successful eIDAS 2 certification

Once Build38 was deployed, the company obtained eIDAS 2 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 European Union (EU) for online identity platforms.

Pedro Hernandez, CSO & Co-Founder BUILD38

>Collaborating closely with the foremost European ID Wallet provider, has been a transformative journey for us at Build38. 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 have 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 immense 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 the pursuit of robust and secure digital identity solutions_

About Build38

The Build38 Mobile App Security Platform empowers businesses to effectively counter security attacks targeting their mobile apps. The platform stands out with its advanced Mobile App Self- Protection, cryptography and AI-driven Active App Hardening, and cloud-based Mobile Threat Intelligence.

Build38 streamlines compliance requirements, expedites certification processes, and eliminates the need for extensive security expertise within mobile app teams. It uniquely caters to the rigorous security requirements of various mobile applications, including mobile-first banking apps, SoftPOS apps, digital ID apps, digital wallets, car key apps, eHealth apps, crypto wallets, and many other application types.

Trusted by industry-leading mobile app companies, the integrated, yet modular, system guarantees zero-trust security across the entire mobile technology stack, encompassing the app, network, and backend infrastructure.

For more information, visit www.build38.com.