SECFENSE + BNP PARIBAS

Case Study

BNP Paribas – Passkeys Implementation Without Interfering with Applications

About the client

BNP Paribas is one of the largest financial institutions in Europe and the leader of the banking market in Poland. The bank serves millions of individual and corporate clients, managing a complex IT environment resulting from numerous mergers and acquisitions.

Each technological change at BNP Paribas must meet strict compliance requirements with internal banking regulations and regulations (including PSD2), as well as ensure operational stability and security - with full availability of services to customers.

Challenge

The project assumed the implementation of authentication **passkeys** in the application **GoOnline Business** without interfering with the existing banking application code. Key requirements included:

- Increasing resistance to phishing and improving customer security.
- Simplify the login process and improve user experience.
- Strengthening compliance with financial sector security standards by implementing additional phishing-resistant mechanisms.
- Full adaptation to existing infrastructure and processes.
- Providing a short and predictable implementation time.

Why Secfense

- **Trust from 2021:** BNP Paribas is the first corporate client of Secfense (cooperation started in 2021) and since then Secfense has been providing protection to the bank's applications.
- **No interference with applications:** Passkeys were implemented without modifications to the front-end of the application, thanks to the use of **User Access Security Broker** and content adaptation.
- **Support for complex architecture:** Integration with extensive infrastructure including multiple sources of identity, various login methods (SMS, tokens, mobile applications) and its own SAML implementation.
- **Security without compromise:** The new authentication mechanism ensures resistance to phishing and compliance with the highest banking security standards.
- **Test flexibility:** The solution enabled safe testing in the Friends & Family environment using the mechanism **opt-in lists**. Thanks to the lists, we can easily indicate which users will get a chance to try the new login method and which will not see any change from the current status.

Implementation process

Stage 1: Preparation and piloting

- **Environment analysis:** The analysis confirmed that it was possible to integrate with the existing authentication process centered around the SAML protocol without requiring any changes to the application code.
- **Content adaptation:** All frontend elements related to passkeys were provided by Secfense and dynamically injected at the load balancer layer.
- **Safe tests:** An opt-in database was created, which allowed individual users to be included in tests without affecting the work of others.

Stage 2: Friends & Family phase

- The test environment was prepared in less than 3 months from the start of the project.
- The use of content adaptation allowed for the dynamic delivery of elements supporting passwordless login without interfering with the logic of the secured applications. Such control allows you to easily decide who will see specific content.
- Initial passkey logins were enabled in the GoOnline Biznes application without disrupting the experience for other users, thanks to the use of an opt-in list mechanism. This allowed for precise management of the test group, monitoring of their experience, and collection of feedback.
- The entire process was carried out in accordance with BNP Paribas' internal security procedures.

The most important challenges

- Integration in a distributed application: The need to work at the interface of various technologies and components provided by independent suppliers.
- Dynamic user management: Selective inclusion of users in tests in accordance with the bank's best security practices.
- Adapt to multi-tier infrastructure by working with distributed domains and heterogeneous systems inherited from previous mergers.

Results

- Preparing the environment for the UAT (User Acceptance Tests) phase in less **than 3 months**.
- **Zero changes to the application code** – the implementation took place directly through the existing reverse proxy, using an additional IDP component and content adaptation to support passwordless authentication with FIDO2.
- **Full compliance with regulations** and the bank's security policy.
- **Leadership position:** BNP Paribas became the first bank in Poland to implement passkey authentication and one of the first in Europe.

Business Case

The economic analysis showed:

- **6x lower costs** support authentication using passkeys compared to traditional methods based on passwords and SMS.
- The costs of migration and maintenance of passkeys infrastructure are significantly lower than the costs of maintaining traditional methods.

Summary

Thanks to the use of Secfense technology, BNP Paribas Bank Polska was able to:

- **Improved authentication security** to a phishing-resistant level.
- **Optimized user experience**, eliminating the need to use passwords and SMS codes.
- **He gained a market advantage**, as the first bank in Poland to offer passkeys login.
- **Reduced operating costs**, achieving multi-million savings.

SECFENSE + BNP PARIBAS

SECFENSE

www.secfense.com