UK high street bank builds trust and security into every payment experience with nCipher HSMs

As financial crime becomes more common and sophisticated, banks and financial services companies are constantly working on better ways to combat fraud, from installing the latest technology to notifying customers when something isn't right. This, together with ensuring its customers' money is kept safe and secure is at the heart of the business of a major UK high street bank.

The revised Payment Services Directive (PSD2) is designed to improve consumer protection, make payments safe and more secure and drive down the costs of payment services. PDS2 regulates all payment service providers completing a payment in EU member states and applies to businesses around the world.

In order to improve security and reduce fraud, PSD2 mandates Strong Customer Authentication (SCA). Put simply this means that more checks will be put in place for customers using digital banking, buying something online, or making contactless payments.

THE BUSINESS CHALLENGE

The bank needed to put in place a strong customer authentication mechanism that would meet PSD2 requirements to reduce the potential for online fraud. It would need to implement a strong two factor authentication (2FA) system which would force more than 300,000 digital banking services customers to confirm their identity and transaction details, quickly, simply and cost effectively.

TECHNICAL CHALLENGE

One of the changes under PSD2 is that SCA requires the inclusion of both the transaction amount and the payee in the authentication process. The inclusion of transaction data in the 2FA process means the data must be encrypted to ensure it is secured and protected from hackers or malicious actors. The solution would also need to operate in real-time, with no degradation in the speed of service visible to the end user.

SOLUTION

The bank issued its digital banking customers with an upgraded smartcard reader with quick response (QR) code functionality that they would use to login, authorize payments or make administrative changes. The card readers have a full display and scanning functionality, rather than the traditional challenge/response type card readers.

The online banking application displays a QR code that includes the encrypted transaction data. The customer scans the QR code with the smartcard reader which then shows the details of the transaction. If the customer is happy with what they see they enter the smartcard PIN. The reader then displays a response code that is entered back into the online banking application. The response code is then verified and the transaction authorized.

In order to protect the transaction data throughout this process, the card reader needs to be verified and the transaction data encrypted to ensure that it cannot be tampered with at any stage during the process.

Each of the smartcard readers is embedded with a public key and the data displayed in the QR code is encrypted with the associated private key. This means that the QR code cannot be read by a standard QR code scanner, only a bank-issued smartcard reader with the correct public key.

"We have been a customer of nCipher for many years now, with nShield HSMs being the HSM of choice to protect the bank's cryptographic keys and processes. By deploying WSOP we were able to make use of our existing estate of HSMs and provide an avenue to encrypt and sign transaction data in a way that met PSD2 requirements."

"The support offered by nCipher and its professional services team was second to none, helping us develop a customized, bespoke solution that met both the bank's needs and the demands of PSD2 SCA. The nCipher team was both thorough and responsive making this a robust, quick-to-deploy strong 2FA solution."

The bank already had an estate of nCipher nShield hardware security modules (HSMs) that it uses to protect the bank's cryptographic keys and processes. It would use these same FIPS 140-2 certified HSMs to store and protect the private keys used to sign the transaction data displayed in the QR code together with nShield Web Services Option Pack (WSOP).

WSOP delivers access to nShield HSMs, no matter where they reside, providing a REST API between applications requiring cryptographic key and data protections services. It provides a simple, seamless interface between the smartcard readers and the nShield HSMs, without the need to install a client. This takes away the difficulties that can be presented by software installation on embedded systems such as the card readers. And without the need to license hundreds of thousands of clients, it was also a cost effective solution. Set up and deployment was quick and easy with the help of the nCipher Professional Services team. The bank required a bespoke modification to the off-the-shelf WSOP which was developed and built by the professional services team, working hand-in-hand with members of the bank's team throughout the project.

RESULT

The bank was able to offer its more than 300,000 digital banking customers a SCA option that complied with PSD2, helping protect their businesses from fraud and cyberattacks. Because of the high throughput of the nShield HSMs the transaction authentication process occurred in real-time, making it a smooth, seamless process for the end user. The customized off-the-shelf solution was much cheaper and faster to deploy than the other options available and considered by the bank.

Business challenge

Provide a Strong Customer Authentication (SCA) two factor authentication (2FA) solution to meet PSD2 requirements

Solution

- nShield Connect HSMs
- nShield Web Services Option Pack (WSOP)
  - Highly accessible connection between cloud applications and HSM services
  - Simple interface, easy integration
  - Reduce costs and set-up time
- nCipher Professional Services team

Result

A real-time strong authentication solution that was easy to deploy and frictionless for the end user

ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. **www.ncipher.com**

N CIPHER
AN ENTRUST DATACARD COMPANY