White Paper

Utimaco Hardware Security Modules in the Age of PSD2

Introduction

Europe's new Payment Service Directive 2 (PSD2) regulation aims to usher in a much more customer-centric and modular banking system. Under PSD2, the customer — not the bank — is the owner of the customer's banking information. Furthermore, this new regime will bring with it new financial entities, who will handle consumer banking information and transactions. Adding more players to the banking ecosystem, however adds more potential security vulnerabilities.

Crucial to the technical implementation of PSD2 are the Open Application Program Interfaces (API)s by which consumer account information can be accessed, and transactions initiated, on behalf of the consumer by third person parties (TPPs). Currently, no single industry-wide solution has been adopted for securing the potential weak links introduced by these TPPs and the Open API ecosystem as a whole. Regardless of what specific solutions are selected for implementing Open APIs, the challenges of maintaining the confidentiality, integrity, and availability of customer financial data in the new world of PSD2 will require the high quality cryptographic material, physical security, and other capabilities of Hardware Security Modules (HSMs). HSMs will be part of any solution which secures the Open API-powered banking of the future, in much the same way they serve as the security linchpin for banking and finance today.

The Potential Benefits of Open APIs

By decoupling a customer's banking information and transaction initiation from the bank, PSD2 and its Open APIs open the door for TPPs to aggregate that data and functionality into a single mobile or web app. More importantly, Open APIs actually encourage this re-aggregation across all of a customer's accounts, regardless of bank. Here are some of the potential benefits for consumers:

Holistic and automated spending, saving, and even investment advice for all accounts. Having the complete picture of a person's finances can allow TPPs to better recommend financial products or even lifestyle tips which would help that consumer achieve savings, retirement, or near-term financial goals.

Continuous, automated comparison of financial product offerings. The electronic aggregation and constant updating of a consumer's financial information makes it possible to easily shop around for better loan or credit card rates without the customer having to fill out paperwork.

Integration of accounting and services into online banking. Since all financial activity across all accounts from all institutions can be viewed and analyzed in one place, bookkeeping becomes much more streamlined, as paperwork records will no longer have to be retrieved and compiled manually.

Increased competition in the financial industry, leading to better pricing and improved customer service. One of the chief aims of PSD2 is fundamentally decentralize banking, and create a much more innovative, modular and open marketplace for financial services. Online-only banks, fintechs, and the new TPPs envisioned and defined by PSD2 (see below) will collaborate and compete with each other as well as with established banks.

New Tech, New Entities

Central to this vision of a less centralized financial industry are the roles played by two types of TPPs defined by the PSD2:

Account Information Service Providers (AISPs): An AISP is an entity which obtains information from a bank (e.g. current balance, transaction history) on behalf of a customer, utilizing the Open APIs. AISPs cannot initiate transactions.

Payment Initiation Service Providers (PISPs): A PISP initiates transactions on behalf of a customer, using the Open APIs to send the transaction request to the appropriate bank and account from which the funds must be transferred. PISPs cannot obtain account information from a bank.

It's important to note that the display of account information and the ability to initiate transactions, normally combined in the mobile bank apps and web banking portals provided by banks, are separated and assigned to two different types of TPPs by the PSD2. Established banks, however, can continue to offer both capabilities.

Under PSD2, both kinds of TPPs will join the banking ecosystem already consisting of banks, customers, fintechs, and regulators.

Open APIs, Interfaces, and Security

Article 27(2) of the draft Regulatory Technical Standards (RTS), which documents the requirements for the interfaces banks must provide TPPs, describes two ways banks can provide TPPs the interfaces they need to obtain account information and initiate payments:

Dedicated interface: banks can create an interface solely for TPPs. The data transferred via such a dedicated interface must conform to the ISO 20022 standard, already widely used for exchanging electronic messages between banks and other financial institutions.

Customer interface: Alternatively, banks can opt to use the existing customer interface (e.g. web or mobile application) for TPPs as well as customers. In this scenario, however, the TPP, not the customer, authenticates itself to the bank.

Each type of interface has its advantages and drawbacks when it comes to security.

Dedicated interfaces require banks to create, maintain, and secure an additional interface, increasing the attack surface. On the other hand, using the ISO 20222 standard for electronic message formatting allows financial institutions to use an existing, vetted, and well-understood technology (and therefore codebase).

Since the customer interface option simply reuses an existing interface, banks which choose this route won't have to design, implement, and secure another interface. The customer interface option, however, essentially shoehorns a new, code-driven process into an interface originally designed for human use, potentially causing pain points down the road.

How to Handle Authentication?

No matter which of the two types of interfaces banks choose to offer TPPs, the TPPs will still have to authenticate themselves to the banks, just as customers will need to authenticate themselves to the TPPs. Because they act as financial "middlemen", TPPs will add further complexity to electronic authentication in the financial industry.

With the aim of reducing the opportunities for payment fraud, the RTS demands both TPPs and banks perform Strong Customer Authentication (SCA) when a user requests their account information or attempts to initiate a payment. This SCA requirement demands that two independent authentication methods, such as username/password credentials in addition to biometrics, be used.

There are three models under consideration for performing authentication (including SCA) between a user and the bank through a TPP:

Embedded: Under the embedded authentication model, the user enters his credentials for the relevant bank account into the TPP's application, and that application forwards him to the bank to verify.

Redirection: Utilized by the card payment protocol 3-D Secure, this model has the TPP's application redirect the user from that app to the bank's app solely for authentication. After the user has authenticated, she is sent back to the TPP's app.

Decoupled: This model is a variation of the redirection model, but instead of the user being sent to a bank for authentication, the user is redirected to what's known as an Identity Provider, which performs the actual authentication.

Hardware Security Modules (HSMs) can play a crucial role in providing the root of trust for all three of these models.

For the embedded model of authentication, HSMs can be utilized to cryptographically sign the published app used by the TPP, proving both the authorship and integrity of the TPP's app to the user. Code signing can thus guarantee to online app marketplaces (such as Google Play or Apple's App Store) and end users that the TPP's app is legitimate. HSMs could also be used as the root of trust at both the bank and TPP, guaranteeing that the TPP's app doesn't pass along the user's authentication credentials to a malicious party masquerading as the user's bank. Lastly, HSMs can also be employed to strongly encrypt all data, including the user's credentials, passed between the TPP and the bank. Only HSMs can perform this encryption while also providing the physical security necessary to keep encryption keys and other critical cryptographic data safe from exfiltration or alteration.

On the other hand, if the redirection model is employed, an HSM at the bank can serve as the root of trust for that institution, proving the bank's identity to both the TPP and the user. This will in turn prevent the customer from being redirected to a malicious credential phishing site. Just as in the case of embedded authentication, HSMs used for redirected authentication can also perform code signing of the TPP's app in addition to encryption of session data passed from the bank's app after successful authentication to the TPP's app.

The decoupled authentication model introduces yet another entity, the Identity Provider (IdP) which provides authentication services. The IdP must be trusted by both the TPP and the user. HSMs can serve as the root of trust for that IdP just as they can for the bank and TPP. Since credentials, tokens and other authentication information must pass between the IdP, TPP, user, and bank, HSMs can provide the high-quality random encryption keys used to encrypt all the traffic between these four parties, as well as performing the actual encryption and decryption of that traffic.

Why HSMs Can Fulfill PSD2's Key Security Requirements

As a robust, integrated hardware, firmware, and software solution, HSMs deliver many essential security capabilities in one package:

Random Number Generation: Session keys, authorization tokens, and one-time passwords require a high level of randomness. Only HSMs with advanced random number generators (RNGs) based on true physical noise will be able to guarantee the confidentiality of sensitive financial data in transit and at rest.

Audit Trail: By time stamping all operations, HSMs provide verifiable security to satisfy financial regulators and investigators.

Encryption: HSMs are able to perform the encryption and decryption of sensitive data within a secure hardware zone, ensuring the confidentiality and integrity of the data before it is released onto the network and sent to a bank, TPP, or IdP. HSMs also securely generate the cryptographic hashes used for code and document signing.

Code Signing: Cryptographically signing identity certificates, application source code, and the published application binaries safeguards the integrity of the software code which ultimately will be used to implement the Open API ecosystem.

Why PSD2 Will Rely on Utimaco HSMs for Implementation

As the leading vendor of HSMs, Utimaco supplies devices which feature excellent physical security (including tamper resistance and tamper-evident construction), and conformance to rigorous security and crypto standards:

- Utimaco's RNG meets the requirements for a DRG.4 random number generator, as specified by AIS 31.
- Every Utimaco HSM is certified to Level 4 of the FIPS 140-2 standards for cryptographic modules.
- The CryptoServer CP5 HSM from Utimaco is the first HSM to obtain Common Criteria EAL4 AVA_VAN.5 approval according to eIDAS Protection Profile EN 419 221-5.

As we explained above, the security and success of PSD2 and its Open APIs ultimately rest upon verifying the digital identities of all the parties involved: banks, customers, TPPs, and IdPs. Utimaco HSMs have a proven track record of keeping crypto keys and digital identities safe. Every day we are relied on to serve as the critical root of trust by generating, issuing, and validating digital identities.

The full implementation of PSD2's Open APIs might use any security solution ranging from Public Key Infrastructure (PKI) to blockchain to eIDAS. HSMs from Utimaco are flexible and robust enough to handle each of these. We work with a network of partners to form a team fully equipped to deliver whatever solution is needed to enable the future of open banking.

About Utimaco

Utimaco is a leading manufacturer of HSMs that provide the Root of Trust to all industries, from financial services and payment to the automotive industry, cloud services to the public sector. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions.

Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 200 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit https://hsm.utimaco.com

Would you like to try out our HSM or implement new algorithms yourself?

Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product.

The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.

Register for free: https://hsm.utimaco.com/downloads/utimaco-portal/hsm-simulator