NFC on Apple: technical challenges, opportunities and preparations for banks and fintechs

7 juillet 2025

The opening up of NFC on Apple's iOS devices represents a major turning point in the mobile payments ecosystem, particularly for card issuers and fintechs looking to offer alternative solutions to Apple Pay. However, this opportunity brings with it significant technical challenges that need to be considered, notably involving technologies such as Secure Element (SE) and Host Card Emulation (HCE), as well as constraints related to certifications and API access.

Understanding the differences between SE and HCE

In mobile wallets, two different architectures are possible: Secure Element (SE) and Host Card Emulation (HCE).

The Secure Element (SE) is a hardware component built into smartphones, designed to protect sensitive information such as card details and cryptographic keys. SE-based solutions, such as Apple Pay, use a tamper-proof environment isolated from the phone's operating system and other applications to carry out transactions, guaranteeing a high level of security. This technology provides strong isolation of critical data.

Host Card Emulation (HCE) is a software solution that virtualizes payment card functionalities without the need for a dedicated Secure Element embedded in the smartphone. In an HCE architecture, payment data is managed via cloud solutions, and security relies mainly on temporary keys (session keys) and tokenization mechanisms. Tokenization is the process of replacing sensitive data, such as a bank card number, with a unique identifier (token) that can only be used in a specific context. In the context of HCE, this mechanism limits the risk of data compromise by ensuring that information stored and transmitted cannot be exploited outside the intended environment. Session keys are dynamically generated for each transaction and renewed regularly to minimize the risk of compromise. In addition, intrusion detection systems are often used to monitor the integrity of HCE sessions, guaranteeing enhanced security against potential attacks. Google Pay is an example of this approach, which is more flexible but potentially presents higher risks than OS-based solutions.

The HCE (Host Card Emulation) approach is considered more flexible than SE (Secure Element) based solutions for several reasons:

- Easy deployment: Unlike solutions based on a physical OS (such as a SIM card or secure chip embedded in the phone), HCE does not require cooperation with hardware manufacturers, mobile operators or banks to integrate a payment solution. This means faster adoption and greater ease of implementation.
- Extended compatibility: HCE solutions work on a wide range of devices, regardless of the presence of a specific OS, whereas OS-based solutions require compatible hardware and may be restricted to certain manufacturers or operators.

- Simplified software updates: Since data and security mechanisms are mainly managed in the cloud, it's easier to deploy security updates and functional upgrades without relying on hardware modifications or new SIM cards.
- Cloud-based approach: Using cloud storage for payment data and authentication enables centralized, dynamic management, whereas the OS relies on more rigid local storage.

However, this flexibility comes at a cost in terms of security: unlike the OS, which is a tamper-proof hardware component, the HCE relies on a software environment, potentially more vulnerable to attacks (malware, data interception, etc.). This is why mechanisms such as tokenization and the use of temporary keys are put in place to reinforce security.

In Europe, Apple has opened up its NFC, but in a limited way to HCE, excluding the Secure Element for third-party applications and reserving this access solely for its ApplePay service. Security is then managed via the Secure Enclave, offering a secure zone for HCE outside the Secure Element. This has a significant impact on the security of alternative payment solutions and may limit their use, notably by excluding cases such as offline transactions, which require the presence of an OS to store information that cannot be transmitted to cloud servers. On the other hand, HCE offers interesting prospects in terms of flexibility, rapid integration and wider deployment.

Technical opportunities and challenges for banks and fintechs

The opening up of NFC on iOS is enabling players such as banks, fintechs and third-party payment service providers (TPPs) to develop their own mobile wallet solutions for proximity payments.

This also paves the way for NFC to be used by sovereign unified solutions such as EPI's Wero wallet for instant payments (IP), the Euro Numérique, and even services linked to digital identity and the future European wallet.

However, implementing an alternative wallet to the main xPay services such as Apple Pay, Google Pay, and Samsung Pay also involves complying with several certification and compliance requirements to be met in HCE applications to minimize the risk of fraud.

For an HCE-based application, the following points must be taken into account:

- Protection of sensitive data: unlike an OS-based solution, where information is securely stored in a dedicated hardware element, an HCE solution relies on software mechanisms and renewable session keys, shared between the client application on the device and the server in the cloud. For example, payment data is encrypted in transit

and at rest using the AES-256 algorithm, and secure communication protocols such as TLS 1.3 are used. Dynamic authentication measures are applied for each transaction, guaranteeing a high level of security. These include end-to-end encryption of transaction data, strong user authentication, and strict management of application permissions.

- Compliance and certification: Every payment application must be certified, passing security assessments such as those required by EMVCo and PCI, as well as the certification processes imposed by payment schemes such as Visa and Mastercard. These validations are carried out by duly authorized independent laboratories. These are all aspects that banks need to consider when launching their own solutions. Added to this are Apple's validation requirements for placing the application on the App Store, which must comply with Apple's strict guidelines for security, privacy and user experience. The validation process includes an in-depth assessment of sensitive data management mechanisms, authentication protocols and compliance with App Store privacy rules.

- Secure Element management: Access to the Secure Element is currently excluded by Apple for the European market, which means that certain additional security features are not available to third-party players. This is a major limitation for applications requiring offline transactions or enhanced data isolation. Note that Apple has opened up access to the SE for certain countries, such as the USA, the UK and Australia.

- Tokenization architecture: Token management (tokenization) is fundamental to minimizing the risk of exposure of sensitive data. Tokens are generated, stored and secured in dedicated environments that prevent unauthorized access. In an HCE architecture, tokens are often stored in the cloud, secured by advanced encryption mechanisms and accessible via secure protocols, whereas in an SE-based architecture, tokens are stored in isolation in the device's hardware, guaranteeing a superior level of security. Efficient integration with a TSP (Token Service Provider) reduces potential fraud vectors.

Opportunities and strategies for the future

Opening up access to NFC on iOS is a long-awaited development, finally offering banks and fintechs the chance to offer new, independent and unified customer services, bringing greater diversity and innovation.

Of course, this HCE management is already well known in the Android world, which has been using it for several years. But on iOS, the only way to make payments was via ApplePay exclusively. This meant having to find alternative interaction solutions, such as QRCode, when the company wanted to bypass ApplePay and avoid the fees imposed by Apple.

For solution providers, the fact that they now have access to Apple's NFC enables them to create unified customer journeys between Android and iOS. It also opens up the possibility of setting up interactions for new services on iOS, such as eID (Digital Identity), Euro Numerique, etc.

However, the technical and compliance requirements associated with the use of HCE make careful planning necessary, both in terms of integration into the banking IS environment, and in terms of customer experience, particularly with the bank's application.

In particular, just because banks are already feeding xPay (ApplePay, GooglePay, SamsungPay, etc.) with customer card tokens, this doesn't mean they can immediately manage a dedicated payment application. All these xPays have been developed and certified in compliance with EMV and card network requirements. They have been tested and validated by accredited laboratories. For banks, developing their own payment application means taking on these tasks and responsibilities themselves.

Another issue for banks is whether or not to integrate this payment functionality with the bank's own banking application. This is a highly structuring choice, both in terms of user experience and additional services, and in terms of solution upgrades and maintenance. For some banks, it's preferable to have an independent application, while for others, the choice is to integrate it into the banking application. There are advantages and disadvantages in both cases, but you need to weigh them up carefully to define the right strategy for your bank.

To take full advantage of this openness, issuers should consider teaming up with experienced partners, such as companies specializing in mobile security and tokenization.

In particular, the support of expert consultants with excellent knowledge of technological, business and compliance issues, combined with an in-depth understanding of the differences between HCE and SE, is essential to developing innovative payment and even digital identity solutions that meet security and user experience expectations. Key topics to consider:

- Details and training on xPAY (SE, HCE, ...)
- Tokenization training
- Audit and analysis of the bank's specific IT infrastructure,
- Identification of potential discrepancies and recommendations,
- Analysis of opportunities and constraints depending on the type of implementation and integration with the bank's application and services,
- Support in finding potential partners (RFI-RFP)
- Analysis and definition of suitable customer paths for the bank (provisioning, revocation, double-tap and FaceId, default application on iOS, etc.)
- Analysis of opportunities and customer marketing arguments to differentiate from ApplePay
- Business model and ROI analysis, compared with ApplePay fees
- Project plan support (POC, implementation project, deployment, etc.)

The opportunities are immense, but it's crucial to be well supported and to ensure that technical challenges, certifications and security requirements are fully understood and anticipated. Acting now will enable issuers to position themselves as leaders in an increasingly competitive payments market.

EESTEL's experts are on hand to answer any questions market players may have, and to support them in their projects.

Contributors

- *Author : Arnaud Crouzet, President of EESTEL, Fime/Consult Hyperion*
- *Reviewers : Christian Mouton, EESTEL, AEMAA Innovation*