Enabling offline payments in an online world

Ensuring trust in scalable offline solutions

Researched and written by

LIPIS ADVISORS

Sponsored by

crunchfish
CONNECT AND PAY. ALWAYS.

About Lipis Advisors

Lipis Advisors is a leading strategy consultancy specializing in the payment sector. Lipis Advisors staff are experts on payment systems, services, and strategy, as well as the underlying technologies that support payment infrastructures. Lipis Advisors advises on all forms of payments, including ACH payments, real-time payments, card payments, cheques, mobile payments, online payments, and RTGS/wire payments.

To learn more about Lipis Advisors, please visit **www.lipisadvisors.com**

About Crunchfish

Crunchfish is a deep tech company developing a Digital Cash platform for Banks, Payment Services and CBDC implementations and Gesture Interaction technology for AR/VR and automotive industry. Crunchfish are listed on Nasdaq First North Growth Market since 2016, with headquarters in Malmö, Sweden and with a subsidiary in India.

To learn more about Crunchfish, please visit **www.crunchfish.com**

Authors

Bonni Brodsky is a managing consultant at Lipis Advisors.

Anurag Dubey is a senior consultant at Lipis Advisors.

We greatly appreciate the contributions from Crunchfish CEO Joachim Samuelsson, CTO Paul Cronholm, CPO Magnus Lageson and senior solutions architect Kristian Sylwander.

crunchfish

AUGMENTING PAYMENTS

Crunchfish have the bold ambition to take a global leadership position within payment technology

Table of Contents

Enabling offline payments in an online world

Ensuring trust in scalable offline solutions

INTRODUCTION

Since we launched our white paper series "Enabling offline payments in an online world" in early 2023, interest in offline payments has grown significantly. This can be seen as a function of expanded interest in CBDCs, with offline use increasingly seen as a core functionality.[1, 2] Additionally, it has emerged in response to the need for greater resilience, convenience, privacy, and inclusivity for digital payment systems that are quickly displacing cash, notably real-time payment systems.

Even with all the increased interest in offline payments, why have they not yet taken off for real-time payments and CBDCs? At present, only UPI in India and Pix in Brazil are beginning to explore offline payment services to make their real-time payment systems more resilient and ubiquitous.[3] Moreover, offline CBDCs have not yet been implemented at scale in any market in which they are live. In part, the tepid implementation of offline payments to date is the result of the unique security and implementation challenges that offline payments pose.[4] There are also significant concerns regarding the maturity and scalability of offline payment solutions that are available today, as well as the ability of solution vendors to meet central bank requirements.[5, 6]

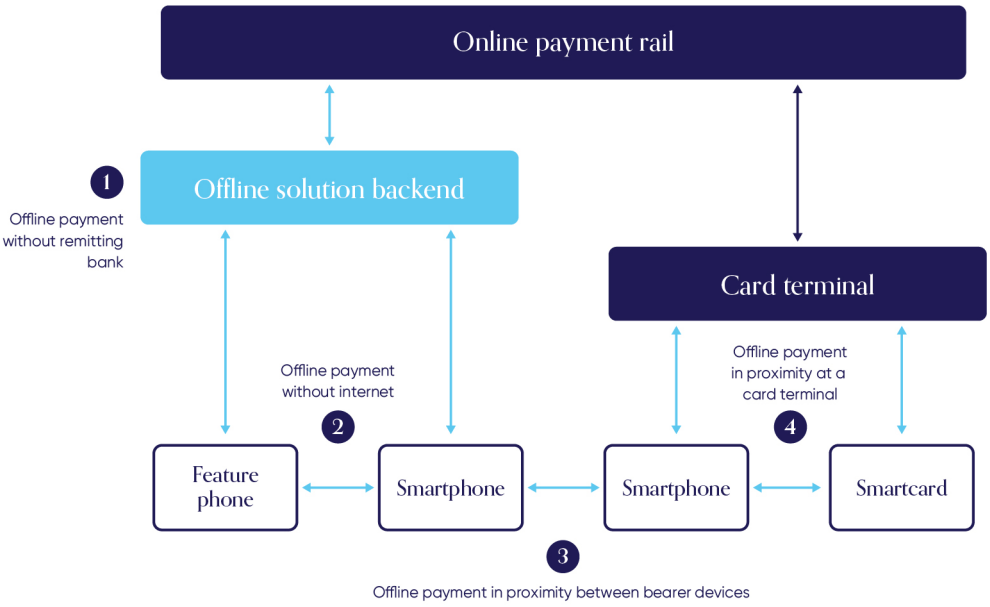
This raises several questions. What are the main issues to address in ensuring trust for offline payment solutions? What implementation approaches are available, and what are their advantages and disadvantages? How should the security of a solution be weighed against its ability to be deployed at scale? And what scheme and regulatory aspects of offline payment system design (e.g., dispute resolution mechanisms, liability frameworks, consumer protection, etc.) must be considered? In this white paper, we address these questions and propose practical guidance for system operators as they consider offline implementation.

[1] https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/
[2] https://www.bis.org/publ/othp64.htm
[3] https://timesofindia.indiatimes.com/gadgets-news/upi-lite-x-for-offline-payments-what-it-means-for-users/articles-how/103534458.cms
[4] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf
[5] https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf
[6] https://www.bis.org/publ/othp79.pdf

ESTABLISHING TRUST: ONLINE VS. OFFLINE PAYMENT SYSTEMS

Online payment systems rely on several intermediaries such as banks, infrastructure operators, payment networks, and payment processors to authorize and process payment transactions. A trusted authority (e.g., a single entity or a distributed network) maintains a copy of the general ledger and updates it continuously. This authority is responsible for validating the transaction, such as whether the funds have already been spent. A secure session is created for each transaction, which enables real-time communication with the authority for validation. Payers are authenticated using methods such as multi-factor authentication or biometric identification to prevent unauthorized access. The transaction is authorized by the payer's payment service provider, which typically involves checking whether the account holder has sufficient funds and conducting real-time fraud assessments.

To enable secure offline payments, a key challenge is how to reach similar levels of trust without involving intermediary parties at the time of payment. Rather, the payee should be able to independently verify the authenticity of the payment. Offline transactions require trust to be established at the level of the bearer instrument given that the funds, balance, or tokens must be locally stored.[7] This represents a significant difference from the online setting. It also emphasizes the additional risk that offline systems carry regardless of how offline functionality is implemented.[8]



1

Offline payments without remitting bank
By reserving an amount in the offline solution backend, the user's remitting bank may be offline at the moment-of-payment.

2

Offline payments without internet
Feature phones and smartphones may connect to the offline solution backend without the internet using USSD, SMS or IVR instead.

3

Offline payments in proximity between bearer devices
Offline payments in proximity bring the ability to pay offline between bearer devices within an amount that has been reserved in the offline solution backend.

4

Offline payments in proximity at a card terminal
At present, offline payments can be made from a card in proximity with merchants taking on counterparty risks. In the future, it will likely be possible for payers to make offline payments using a card by reserving an amount using pre-authorization, eliminating counterparty risks to merchants.

Figure 1 Four ways of enabling offline payments

Source: Lipis Advisors

[7] https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/
[8] https://www.bis.org/publ/othp79.pdf

Payment system operators have unique goals and motivations concerning offline payment system design, and there is no "one-size-fits-all" solution for offline CBDCs or real-time payments. An offline payment solution can, however, achieve the levels of trust required for secure offline payments if the following areas are addressed:

VERIFIABILITY
The payee should be able to independently verify the authenticity of the payment in offline mode.

FINALITY
Once a payment is complete, the receiver must have finality in offline mode to own the transferred funds.

REDEEMABILITY
A bearer instrument holder must be able to convert any balance from their offline balance into their online balance (and vice versa).

TRANSITIVITY
Users should have the ability to spend the received payment amount (fully or partly) in the same offline session without the need to go online.

SECURITY
Offline payment systems must be designed to prevent double spending, ensure the security of funds in the wallet (bearer instrument), and guarantee the total supply in the system remains the same i.e., a client can only add/remove money to/from the system via the deposit/withdraw functionalities provided by the server.[9]

In the next two sections, we consider how these areas can be addressed as well as the different options for implementing trust at each level of offline payment system design: the offline security protocol and the offline trusted environment.

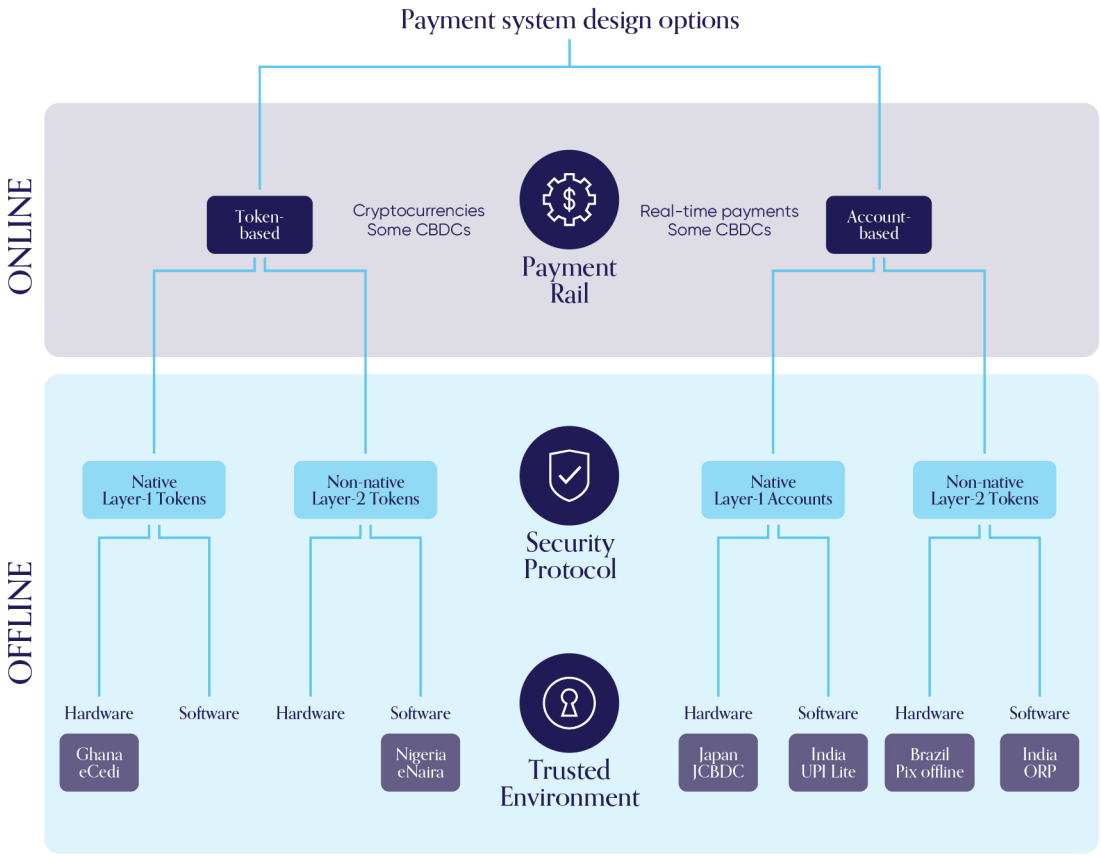


Figure 2 Payment system design options

Source: Lipis Advisors

[9] https://arxiv.org/pdf/2012.08003.pdf

IMPLEMENTING AN OFFLINE PAYMENT SECURITY PROTOCOL

The offline security protocol provides a mechanism through which the authenticity of offline payment can be verified without the involvement of a trusted authority. This is true regardless of whether the offline security protocol is native layer-1, transferring tokens that have been minted online, or as a non-native layer-2 protocol.[10] With consecutive offline transactions, any transferred value is immediately available for future spending, potentially leading to rapid value creation that cannot be easily detected.[11]

Digital signatures have long been a best practice for offline EMV card payments, which rely on different forms of Offline Data Authentication (ODA), enabling a point-of-sale (POS) terminal to securely verify the authenticity of the card.[12] For wallet-based offline payments, payment system operators can take a similar approach by using a two-layer infrastructure that deploys digital signatures with public key pairs at the protocol layer along with PKI certificates to authenticate the offline messages transmitted at the application layer.[13] Crunchfish Digital Cash and Visa's Offline Payment System provide examples of non-native layer-2 solutions using digital signatures and PKI certificates.[14] In India, NPCI recently implemented UPI Lite X, which enables UPI payments between offline wallets also based on this approach.[15] A recent prototyping exercise conducted by the ECB also showed that an offline peer-to-peer solution for a digital euro could potentially leverage cryptographic signatures applied to transaction history to mitigate fraud risks.[16]

IMPLEMENTING A TRUSTED ENVIRONMENT FOR OFFLINE PAYMENTS

Offline implementations that allow for extended offline use must not only protect cryptographic keys from tampering and other attacks, but also offline assets such as the offline balance, risk parameters limiting the frequency, value, or time validity of offline transactions, the integrity of settled transactions that have yet to be reconciled, and user credentials (e.g., password, PIN, biometric data). The BIS and other organizations have identified the use of tamper-resistant Secure Elements (SEs) in a trusted environment as a best practice for offline payment implementation.[17, 18] Hardware-based trusted environments are commonly found in smartcards and on SIM cards as standalone implementations or as device-integrated trusted environments on smartphones. Software-based trusted environments utilize tamper-resistant virtual SEs.[19]

A key question for payment system operators is therefore whether to choose a hardware- or software-based offline solution, with not only security but also scalability and interoperability as important considerations. Hardware-based security is generally well-established in the market and is proven to offer robust protection against various potential threats. However, its use poses scalability challenges when physical components or devices must be updated or replaced. Software-based security, although less mature in the market, is more cost-efficient and scalable. If a security vulnerability is identified, it is typically simpler to update a software-based solution.[20] Frequent reconciliation with the online ledger, the implementation of anti-rollback mechanisms

[10] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf
[11] https://www.bis.org/publ/othp64.pdf
[12] https://www.smartpaymentassociation.com/publications-smart-payment-association/position-papers-smart-payment-association/entry/why-offline-authentication-still-matters-in-today-s-online-payments-world-a-spa-insight
[13] https://www.mdpi.com/2076-3417/12/9/4488
[14] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf and https://arxiv.org/pdf/2012.08003.pdf
[15] UPI Lite X Masterclass, Global Fintech Fest 2023 (Mumbai)
[16] https://www.ecb.europa.eu/pub/pdf/other/ecb.prototype_summary20230526~71d0b26d55.en.pdf
[17] https://www.crunchfish.com/wp-content/uploads/2023/01/Lipisadvisors_WP1_offlinepayments.pdf
[18] https://www.bis.org/publ/othp64.pdf
[19] https://www.v-key.com/products/v-os-virtual-secure-element/
[20] https://www.bis.org/publ/othp79.pdf

for devices, and backend protections such as certificate revocation, can make software-based solutions highly secure.

Several other implementation questions also emerge from this discussion. Should the trusted environment be provided as an integral part of the mobile device, as a standalone Tamper Resistant Element (TRE) on a SIM, or closely integrated with the payment app itself? Until now, there has been limited experimentation in the market around these questions, with the need for greater exploration and discussion.

LEVERAGING THE ONLINE PAYMENT RAIL

There is increased acknowledgment from the market that backend reconciliation is an important mechanism for fostering trust in offline payments. The ECB has indicated that for offline payments using a future digital euro, user devices would be expected to regularly go online, both to account for technical limitations (e.g. available storage on the devices) and to mitigate the risks associated with potential financial fraud.[21] Although the frequency and timing of this may vary across systems in practice, it plays an important role in ensuring the security and integrity of offline payments. For example, once both the payer and payee's bearer instruments have reconciled with the online ledger, the backend provided by the offline solution can confirm whether the data associated with the offline transaction match from both the perspective of the payer and payee as well as whether the offline transactions are reflected in both the payer and payee's bearer instrument.

Certificate factories at the backend allow for the creation and management of digital certificates, including revocation and replacement. Certificate revocation can be used to prevent the continued use of a compromised or invalid certificate, thereby maintaining trust and security within the system. When reconciliation with the online payment rail occurs, a list of revoked certificates can be updated to ensure that the offline solution is kept current on any certificates that have been deemed untrustworthy since the last update. As cryptographic algorithms and technology evolve, newer certificates can employ more advanced security practices, enabling continued trust in the solution.[22]

Last, offline solutions must have mechanisms whereby the trusted application can detect whether the secure storage has been tampered with as well as fraud mitigation measures such as deactivating the wallet until the user is back online. The backend can respond with further measures such as revoking certificates once tampering or manipulation of the device has been detected.

NON-TECHNICAL ASPECTS ENSURING TRUST IN OFFLINE PAYMENT SOLUTIONS

The implementation of a trusted offline payment solution, in any economy, does not happen in isolation. It requires putting in place scheme rules, regulations, and other policies to ensure trust. In this last section of our paper, we consider the non-technical offline payment system design aspects that help to reinforce trust once a solution has been implemented.

SETTING RISK LIMITS

When any new payment method or solution is introduced into the market, it is often initially rolled out with strict transaction limits. This allows ecosystem participants to monitor security vulnerabilities and respond to them before they can cause widespread harm. Contactless payment card payments, for example, were introduced in most markets with lower transaction limits than can be observed today. Value limits have gradually increased but still exist to limit the potential damage from fraudulent activity. For new forms of account-based offline payments or offline CBDCs, a similar approach could be taken. Risk limits could be implemented as time-based for transaction-based restrictions (e.g., value or frequency), monitored, and then reassessed.

[21] https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf

[22] https://www.ibm.com/docs/en/sdk-java-technology/8?topic=interfaces-certificatefactory-class

ESTABLISHING A CLEAR REGULATORY AND LEGAL FRAMEWORK

For offline payment systems, new regulations may be necessary to ensure the safety and security of offline funds for users. A well-defined framework clearly outlining the liability of the solution provider, issuer, and user in the case of fraudulent or erroneous transactions, and conditions for these liabilities, needs to be in place. Liability coverage for assets stored in offline wallets can also enhance trust among users, as they know they are protected against certain losses. Having a clear framework that defines the recourse for users and other ecosystem actors in case of disputes or fraud is essential to establishing trust.

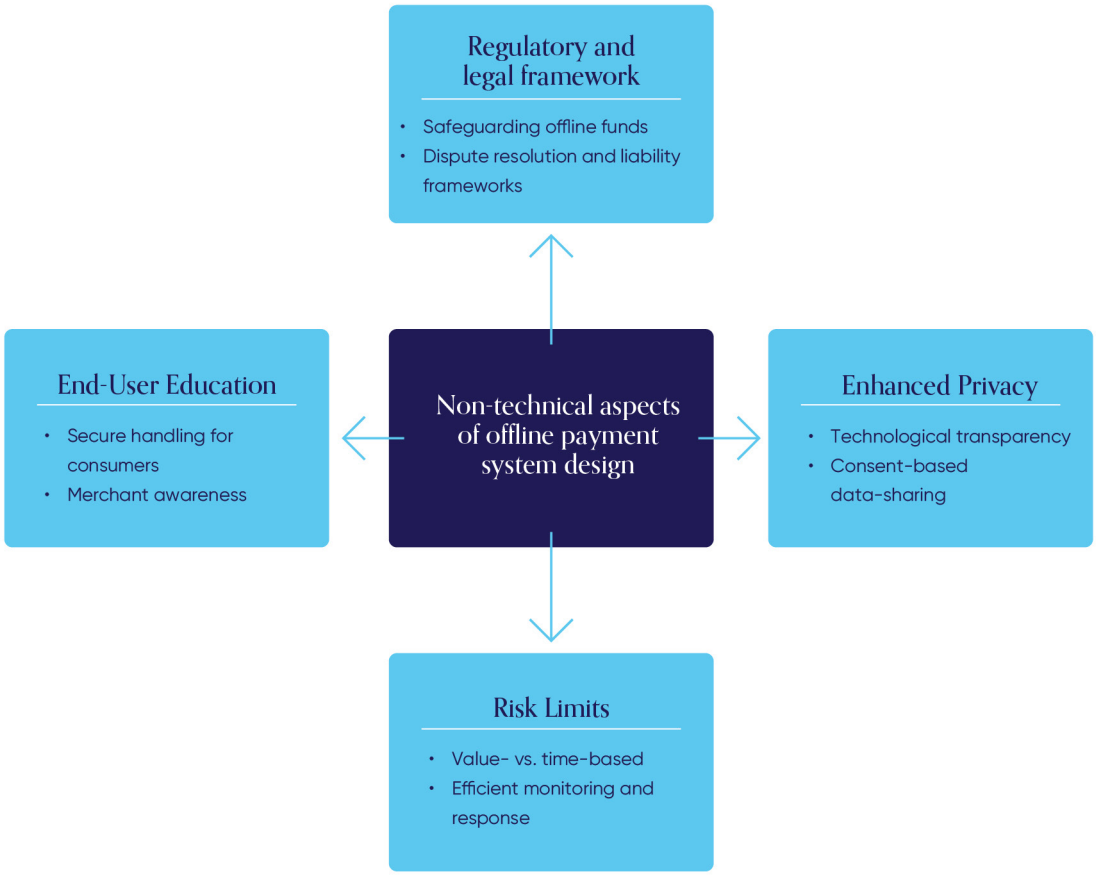


Figure 3 Non-technical aspects of offline payment system design

Source: Lipis Advisors

SAFEGUARDING USER PRIVACY

Safeguarding user privacy is a best practice from a security perspective as it can help prevent the unauthorized use of consumer data in the event of a cyber-attack or data breach and can help mitigate the commercial exploitation of data by solution providers without user consent. In addition, privacy concerns can have a significant impact on users' willingness to use or adopt digital payment methods or services. Data-sharing for value-added services (VAS) should be consent-based. Maintaining transparency about the technology used by the solution, its privacy features, and any known risks can also help reassure users about the safety of their sensitive data.

BUILDING AWARENESS

Given the potential negative consequences that could stem from the inevitable loss or theft of devices, educating end users on the secure handling of private keys and the risks associated with offline transactions is an important aspect of fostering the user trust required for successful implementation. Awareness efforts must also be tailored toward different user segments, and not just consumers. Merchants may perceive the benefits and risks of offline CBDCs or real-time payments to be the same as for offline card payments, with which they may be more familiar. In offline card payments without issuer authorization, the merchant assumes some counterparty risk since the payer may not have the necessary funds to complete the transaction. However, in the case of offline CBDCs or real-time payments, settlement is immediate and final.

CONCLUSION

In a real-world implementation of offline solutions, security and trust is of utmost importance. In this paper, we highlighted the need for using digital signatures and PKI certificates at the level of the offline payment security protocol, weighed the benefits and disadvantages of hardware- vs. software-based trusted environments, and detailed strategies for leveraging connectivity with the online payment rail to mitigate and detect fraud. We concluded with a discussion of non-technical design aspects such as risk limits and liability frameworks, that should be considered to reinforce trust in an offline payment solution.

Looking back on this white paper series, which has covered a range of topics relevant to offline payment system design, a key theme that has repeatedly emerged is the importance of striking the right balance between security, trust, and scalability. No matter how trusted an offline solution is, payment services will not be implemented unless the solution is cost-efficient and scalable. By the same token, no matter how scalable the solution is, payment services will not be implemented, and users will not use the services unless the solution can be trusted.

What is the way forward then for payment system operators in confronting this dilemma? For one, extensive exploration into the various aspects of offline payment system design, not only security, but also privacy, interoperability, and scalability, is required. Further experimentation with different offline solutions, technologies, and providers to obtain more detail into the design trade-offs is also needed. Perhaps most importantly, however, payment system operators must clearly define their motivations, goals, and risk tolerance to choose an implementation approach and solution that is right for their market.

Crunchfish editorial on secure and scalable offline payments for smartphones

It is a challenge to add offline payment capabilities to payment applications on smartphones. The level of security must be increased as offline payments cannot rely on the backend security when making and storing offline payments. For scalability, it is important to be able to deploy offline payment solutions on all devices on which the underlying payment application is used. This editorial describes various hardware- and software-based implementation architectures and discusses whether they are secure and practically suitable for smartphone-based offline payments. It complements the views expressed in our previous editorial on offline payment design choices, which focused on the offline security protocol rather than the offline trusted environment.[23]

Payment applications running on smartphones are implemented in software-based **Rich Execution Environments (REEs)**, which provide high levels of programmability but are not secure enough for offline payment operations. Cryptographic keys and other offline assets such as the offline balance and transaction risk limits are not safe from simple attacks.

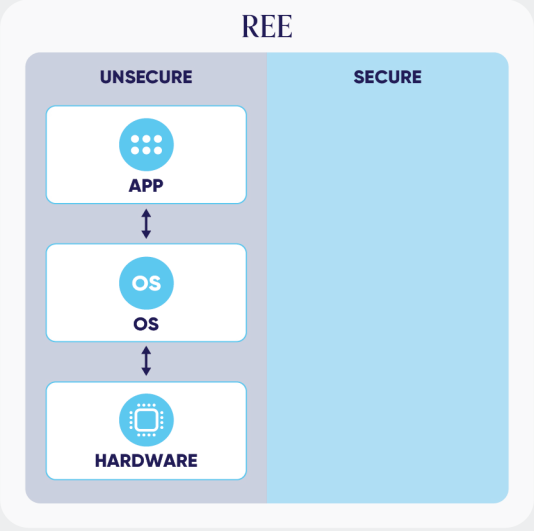


Figure 1 The Rich Execution Environment does not provide the required security for offline payments.

Source: Crunchfish

To be secure, offline payments must be implemented as a Trusted Application (TA) within a Tamper Resistant Element (TRE) that protects the TA with an isolated secure runtime for cryptographic keys and other offline assets. A key consideration for establishing the required additional security for offline payments is the implementation of the TRE. As discussed in Lipis Advisors' white papers and the BIS' recently published handbook on offline payments for CBDCs, it could either be implemented in hardware or software.[24, 25] A TRE implemented in hardware is a Secure Element (SE) whereas a software-based TRE is a virtual SE.

HARDWARE-BASED TRE

A hardware-based TRE could either be a device-integrated TRE in the System-on-Chip (SoC) or as a standalone TRE as an embedded SE or on a SIM/eSIM. **Device-integrated TREs** integrated into the SoC, such as Android Keystore or iOS Keychain, are widely available on smartphones. However, they protect only the use of cryptographic keys and are therefore not sufficiently secure for offline payments as they lack a secure runtime for other offline assets. A simple attack is all it takes to bypass the offline balance and the risk rules.

[23] https://www.crunchfish.com/wp-content/uploads/2023/05/Lipis_WP2_Crunchfish_Enabling-offline-payments_v5.pdf
[24] https://www.crunchfish.com/wp-content/uploads/2023/01/Lipisadvisors_WP1_offlinepayments.pdf
[25] https://www.bis.org/publ/othp64.pdf

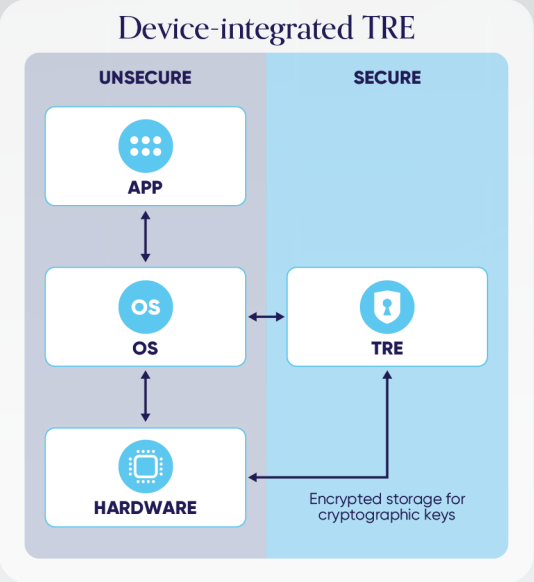


Figure 2 A device-integrated TRE that only handles cryptographic keys is not secure enough for offline payments as the other offline assets are not protected. An offline payment TA on a device-integrated TRE able to handle cryptographic keys and other offline assets is hard to deploy in practice. Source: Crunchfish

Another common way that allows mobile payment applications to increase their security is to use the device-integrated Trusted Execution Environment (TEE) typically delivered by ARM Trustzone. Although is technically possible to write an offline payment TA that can handle both cryptographic keys and offline assets on a device-integrated TEE, device fragmentation in the market makes it difficult to implement. Several challenges emerge:

- Mobile devices use different TEEs that come with their specific operating systems. This means that it would be necessary to implement multiple offline payment TAs to execute on the variety of TEEs.
- The next and harder challenge is how to provision the offline payment solution in the market. Provisioning a TA to a device-integrated TEE is not suitable for third parties because the remote distribution system is not mature. It would be necessary to partner with multiple device manufacturers to get the offline payment TA loaded onto their devices to achieve widespread availability in the market.
- Furthermore, there is currently no support for implementing an offline payment TA on a device-integrated TEE on iOS, which limits its market penetration.

These hurdles make offline payment TAs on device-integrated TEEs hard to deploy in practice. In addition, there are also several known attacks on applications using TEEs, which make them unsecure for offline payments.[26]

Standalone TREs are another type of hardware-based TREs that can provide an offline payment TA with secure runtime and storage for cryptographic keys and offline assets. The commonly available smartcard is an example of a standalone TRE and may be used for offline payments.

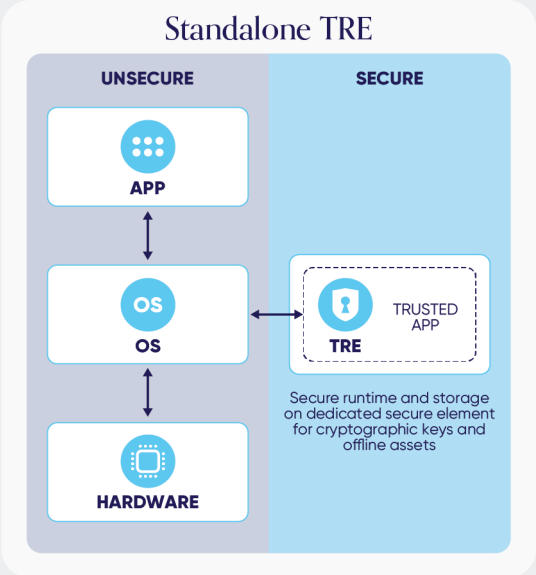


Figure 3 A standalone TRE that provides an isolated secure runtime and storage for cryptographic keys and offline assets that is secure for offline payments. Whereas offline payments on smartcards are available, it is hard to deploy offline payment TAs on standalone TREs in mobile devices in practice due to device fragmentation and limited mobile OS support. Source: Crunchfish

Standalone TREs may also be implemented in a mobile device either as an embedded SE or on a SIM or eSIM. However, provisioning an offline payment TA in a mobile device on a standalone TRE poses similar challenges as in a device-integrated trusted environment. To achieve widespread market availability for a payment

[26] https://ieeexplore.ieee.org/document/9152801

application with offline payment support, there is a need for the payment application provider to partner with a sufficiently large number of device manufacturers or possibly mobile operators if the standalone TRE is implemented on a SIM. There are also additional challenges in manufacturing and distributing the standalone TREs to smartphones. This creates hurdles to bringing mobile payment applications with offline payment TAs on standalone TREs to market.

TRUST GAP ISSUE

A common belief is that hardware-based SEs are always more secure than software-based virtual SEs because of the clarity of security boundaries. However, due to the inevitable separation between the payment app and the hardware-based TRE, there is a gap in the chain of trust between the two communicating endpoints. This can result in potential attacks by replacing either endpoint with malicious ones, or tampering with them and modifying their behavior during runtime. As the TRE does not have full visibility of the payment app and the mobile OS, it cannot determine the identity of the app or whether the app has been tampered with, and has to "blindly" trust the OS and the app.[27]

SOFTWARE-BASED TRE

As noted, software-based TREs on smartphones are based on tamper-resistant virtual machines, also known as virtual SE. They offer the required security for offline payments as they provide the required isolation by a virtualized secure runtime and encrypted storage for cryptographic keys and offline assets. Attackers cannot tamper with the offline payment TA or bypass the protection mechanisms without first breaking the virtual SE itself. Weaker software-based protection solutions that rely on a combination of code obfuscating and white-box cryptography are not sufficiently secure for offline payments. The primary weakness of such solutions is that the cryptography and runtime protection mechanisms run natively on unsecure hardware, which attackers can easily bypass.

Software-based TREs are implemented as **app-integrated TREs**. This means that the offline payment TA resides within a virtual SE that is integrated with the payment app. As the app-integrated TRE is an integral part of the payment app, there is no trust gap, and it provides a consistent level of security for offline payments independent of the device on which it is running. Another key benefit is that the offline payment TA can securely run on jailbroken or rooted devices as a compromised device does not affect the running of the offline payment TA within the virtual SE.

As cryptographic keys and offline assets are stored encrypted on unsecure hardware, offline payment TAs in app-integrated TREs are susceptible to "rollback" attacks.[28] However, offline payment TAs can still be made highly secure for offline payments, if rollbacks are mitigated and reconciliation with the backend is sufficiently leveraged.

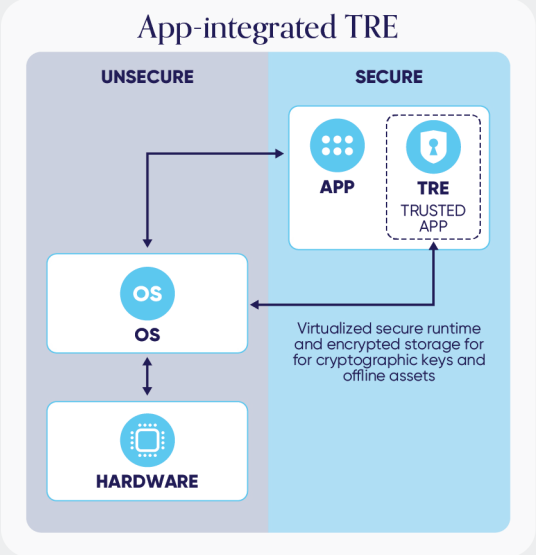


Figure 4 An app-integrated TRE provides a secure environment for offline payments. It provides isolation by a virtualized secure runtime and encrypted storage for cryptographic keys and offline assets. It is highly scalable, as the offline payment TA is deployed and updated with the payment app on all smartphones using app stores. Source: Crunchfish

The offline payment TA can easily be integrated with a payment application with the same flexibility as writing a regular app. It can be deployed and updated on any smartphone together with the payment app using app stores. Altogether, this makes the solution highly scalable and well-suited for offline payments on smartphones.

[27] https://www.v-key.com/resource/most-mobile-authentication-apps-can-be-breached-even-if-hardware-security-is-used/
[28] https://www.psacertified.org/blog/anti-rollback-explained/

CONCLUSION

In summary, offline payments require a much higher security than what is offered by the standard Rich Execution Environment on a smartphone. This higher level of security may be achieved by implementing offline payments as a TA protected by a TRE that provides a secure runtime and storage for both cryptographic keys and other offline assets, such as the offline balance and risk rules. The TRE can be provided either as a hardware-based standalone TRE or a software-based app-integrated TRE.

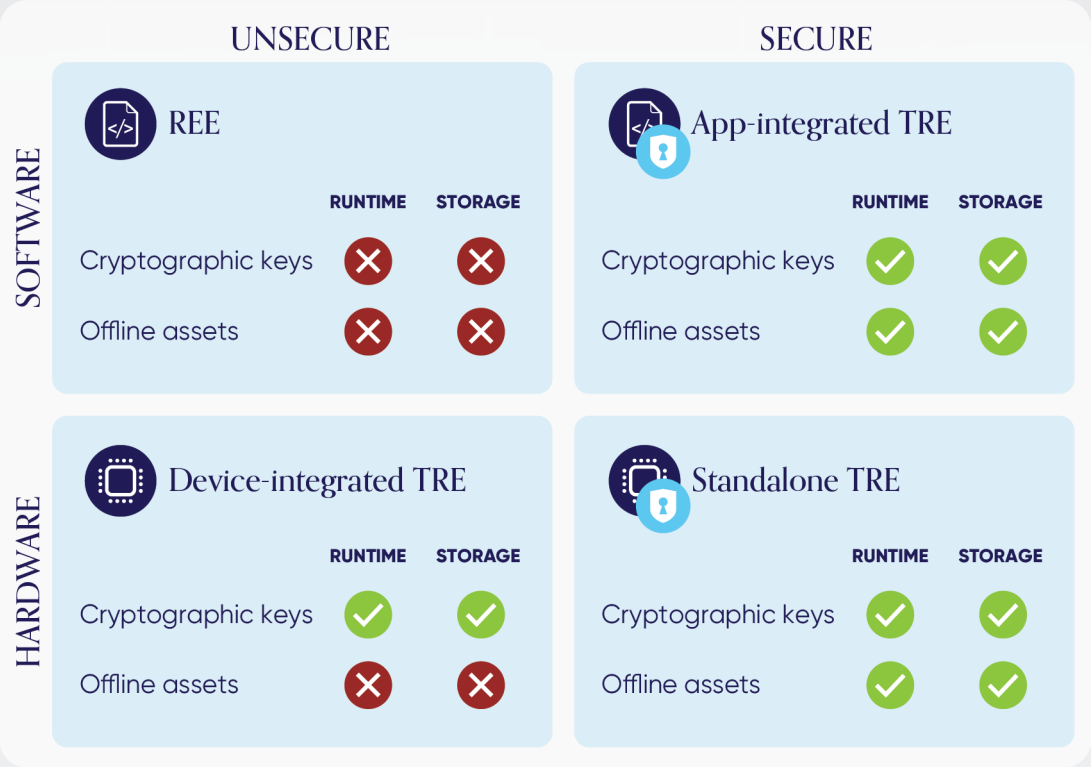


Figure 5 An overview of hardware- and software-based implementation environments for offline payment TA

Source: Crunchfish

Reflecting on our above analysis, the main difference between implementing an offline payment TA on hardware-based and software-based TREs is not the security but the scalability of the offline payment solution. Whereas hardware-based TREs are costly and hard to deploy due to device fragmentation, a key takeaway is that this is not the case for app-integrated TREs. On the contrary, it is a cost-efficient solution that is easy to integrate with the payment applications and deploy and update on app stores for any smartphone.

Crunchfish is pioneering offline payments with its Digital Cash offline payment solution, protected by an app-integrated TRE. As far as Crunchfish is aware, Digital Cash is the only offline payment solution that is both secure and scalable for smartphones available on the market.