E-krona report

E-krona pilot Phase 4

March 2024

SVERIGES RIKSBANK

Table of contents

Glossary

Payment instrument: An electronic device used by the end-user to make a payment, such as a card or mobile phone.

Point of Sale terminal: Hardware solution where the shop accepts payments from payment instruments. Point of Sale (PoS) terminal.

CBDC: Abbreviation for Central Bank Digital Currency. A digital form of central bank money.

Corda: DLT platform on which the e-krona pilot test network is built.

Corda node: Holds and handles wallets.

DLT: Distributed Ledger Technology - distributed storage of information, for example from a transaction. The information is spread among participants in a network instead of being stored in a central location. Members of the network can usually read and, depending on authorisation, add information.

E-krona: Swedish CBDC available to the general public.

E-krona node: Part of the DLT platform hosted and operated by the respective intermediary.

E-krona engine: Node where intermediaries can build their own business logic.

E-krona network: A network consisting of the Riksbank and authorised participants, known as intermediaries, in which the e-krona is distributed and used in transactions. The network is built on a DLT platform called Corda.

Intermediary: An umbrella term for the different types of organisations connected to the E-krona platform. Legal person with the right to act as agent and/or provide e-krona services.

NFC: Abbreviation for Near Field Communication. Technology that enables wireless communication between devices such as payment cards and payment terminals.

Notary-node: Checks to ensure that there is no duplication.

Offline: When communication between payment instruments and e-krona network is not available.

Offline wallet: Found on the payment instrument, such as a payment card.

Online wallet: Located in the intermediary's node.

Wallet: Storage space for e-krona holdings

Shadow wallet: Located in the intermediary's node, it is a mirror of the user's offline wallet. The shadow wallet is the link between the offline and online wallets.

Token: Within the e-krona pilot, a uniquely identifiable digital unit of value that can carry the value of Swedish kronor.

Synchronisation: A measure to reconcile data stored on the payment card with data stored at the intermediary.

1 Summary

In the fourth phase, the focus has been on testing and evaluating whether it is possible to design a secure, balance-based offline solution based on the conditions of the e-krona pilot's test environment.

The solution reserves e-krona for offline use in a so-called shadow wallet in the online system. The payment instrument in the form of a card records the shadow wallet balance and subsequent offline transactions. The actual e-kronas issued by the Riksbank never leave the online system and only change hands when the payment instruments are synchronised. The solution thus differs from the offline solution tested in Phase 2, which was token-based and involved moving copies of the e-krona to the payment instrument.

Three different use cases were tested: funding and de-funding e-krona to the payment instrument, offline payment from card to payment terminal (PoS) and offline payment between two cards. In addition, there was a test of imposing limits on the balance and number of transactions on the payment instrument. As the cards cannot communicate by themselves, mobile phones and apps are needed to link them. The solution was based on the fact that these mobile phones could not be considered secure, which placed additional demands on the ability of the cards and the e-krona system to ensure the integrity of the transactions.

Transferring e-krona to the card is done by the user with a mobile phone app connected to the online system. Loading e-krona onto the card requires trust in the intermediary's systems and processes, as the balance recorded is not technically traceable to the e-krona issued by the Riksbank.

In-store payments were made via a mobile phone that acted as a PoS terminal. Since there was no access to the secure hardware of the terminal, some proprietary security features were implemented to protect the stored transactions.

Based on the fact that mobile phones are insecure components, user-to-user payments require many steps to be considered secure, which compromises user-friendliness. This is a direct consequence of the fact that the cards require a reader in the form of a mobile phone to communicate. The opportunity to reduce the number of steps is considered small in this design.

Payments made offline need to be synchronised so that the balance in the offline wallet corresponds to the e-krona reserved in the shadow wallet in the online system. Depending on the order in which users synchronise, problems may arise from lack of liquidity in some shadow wallets.

Many lessons have been learnt during the project, the most important of which is that a secure and functional offline solution requires a lot of development cooperation work in terms of technology, regulations and processes. Nevertheless, the conclusion is that with the right boundaries and regulatory framework, it should be possible to develop a secure and usable offline solution.

2 The e-krona pilot

Since 2017, the Riksbank has evaluated the possibility of issuing a central bank digital currency to the general public, what would be known as the e-krona. In 2020, an e-krona pilot project was started.1 The work of the e-krona pilot has been aimed at testing different technical solutions and examining different legal aspects in parallel. The aim has been for the Riksbank to learn more about how an e-krona could work through practical work. This report summarises the work and conclusions of the fourth and final phase of the pilot, which focused on integrating secure offline payments into the e-krona pilot environment. There is currently no decision on issuing an e-krona, nor on which technology would be used.

Following the fourth phase of the pilot, the Riksbank's work on the e-krona has entered a new phase. The technical pilot was concluded in October 2023 and the work of analysing the requirements that must be set for an e-krona and the consequences of issuing one, as well as communicating the Riksbank's view of how an e-krona should be designed, is continuing. In parallel, the Riksbank is monitoring international developments. Digitalisation will continue in Sweden and abroad, which will require new payment solutions. An e-krona could be an important addition to the payments market.

The e-krona work focused on by this and previous reports is therefore what is usually referred to as a *retail CBDC*, a central bank digital currency available to the general public. During the previous phases of the e-krona pilot, we have developed an e-krona network in a test environment, in which e-kronas are distributed to end users via Riksbank-authorised participants in the network. We have then gone on to test how an e-krona network could be integrated with the participants' internal systems, how an offline solution could work, how the e-krona could be integrated with existing PoS terminals and what performance challenges the tested solution is facing.

We have also examined how the Riksbank could cooperate with market participants when distributing e-krona to the public. In addition, we have tested the possibilities to promote innovation on the payments market, such as smarter and more efficient ways to pay. The pilot's test environment has also been used for international cooperation such as the Icebreaker project, which explored whether an e-krona could enable more efficient and secure payments between countries and CBDC networks.

[1] The e-krona pilot reports are available on the Riksbank's website, https://www.riksbank.se/sv/betalningar--kontanter/e-krona/.

In the fourth phase, the work of the pilot has been limited to investigating:

- Whether it is possible to design a balance-based offline solution based on the conditions of the e-krona pilot test environment and analyse how secure this could be.
- The security of an off-line solution based on an e-krona specific payment card and an in-store payment terminal.
- The ability to use the existing EMV standard[2] which is the global standard for debit and credit cards.

[2] EMV is the standard developed by Europay, Mastercard and Visa. The standard is currently managed by EMVco, which consists of American Express, Discover, JCB, Mastercard, UnionPay and Visa.

3 Secure offline payments

The balance-based solution developed in the fourth phase of the e-krona pilot shows that offline payments are feasible but that there are security challenges, for example in the case of person-to-person payments. Cash flow problems can also arise when several payments are made one after the other without being synchronised. Limits on the number of transactions or a maximum amount can reduce the risks, but a solution still needs to be found to allow these to be changed without having to distribute new cards.

3.1 Objectives and conditions

The Riksbank's objective in phase four has been to design a secure offline solution with the conditions of the e-krona pilot and then to test and evaluate it. Thus, we have utilised the pilot environment for the e-krona and payment instruments previously developed. In addition, it was examined whether it was theoretically possible to make use of the EMV standard used globally for debit and credit cards, as this is proven and works well.

The e-krona pilot has been developed on a DLT-based system solution built on the Corda platform. The Riksbank and the intermediaries are part of an isolated test network with their own nodes. For the e-krona to work offline, a payment instrument is needed that does not rely on continuous communication with the e-krona system. In this phase, payment cards and mobile apps have been further developed to make this possible. A so-called *Store value solution* has been implemented on the payment card where the balance for offline use is saved.

We have also explored whether it would be possible to offer offline payments using only a mobile phone. However, this was not possible as our assessment is that it was not possible to achieve adequate safety. We therefore chose to base the offline solution solely on cards.

3.2 Overall design

In this phase, we chose to reuse the previously developed pilot environment for the e-krona with unchanged roles for the Riksbank and the intermediaries.

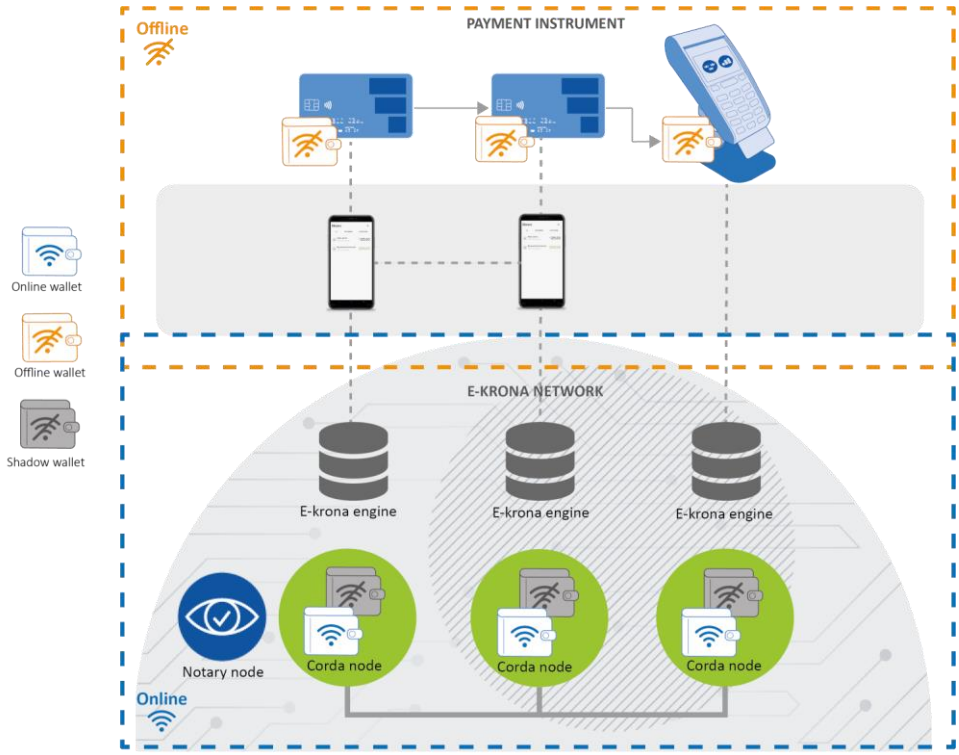


Figure 1. Overall design

Again, the Riksbank is responsible for a notary node where e-krona transactions are verified and settled. Intermediaries provide users and merchants with e-krona wallets, payment instruments and payment terminals. Users should be able to carry out transactions with other users and pay at merchants even when the e-krona network is not available, i.e. offline.

With these basic assumptions, we designed an offline solution based on payment cards and evaluated its security. We used the same cards as in previous phases of the pilot[3].

The difference compared to the previous offline solution was that in phase two the solution was based on tokens with transaction chains stored on an Android mobile phone. In this phase, only the balance and offline transactions are stored on the end user's payment card or in the merchant's payment terminal. The payment instrument that stores the balance and offline transactions is called an offline wallet. In both solutions, phase two and phase four, each user needs an additional wallet type to handle offline payments. In phase four, we call this wallet the shadow wallet, see Figure 2. This means that each user has two wallets in the intermediary's Corda node, the shadow wallet and the regular online wallet. Shadow wallets are used to manage users' offline transactions. For example:

- When the user wants to top up or empty their reserved e-kronas for offline transactions.
- When offline wallets should synchronise all offline transactions.

[3] "Dual-interface" with "NXP P71 Secure Element chip" and the operating system "JavaCard JCOP4"..

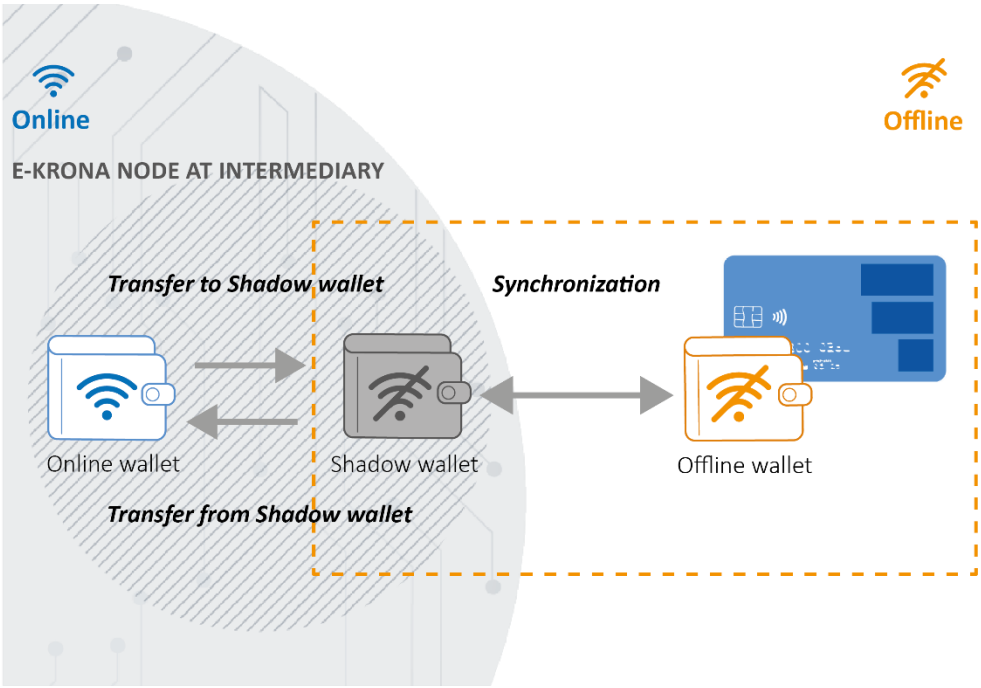


Figure 2. Each user has their own online wallet, shadow wallet and offline wallet.

Security design

The solution is based on managing balances and transactions on what is known as a Stored Value Card. Certificates and various counters are introduced to increase security. The aim was to see what a secure solution for offline payments could look like.

The design and solution relies on the strong protection of the intermediaries' systems (e-krona engines) and cards and the correct management of the systems by the administrators. The design also assumes that PoS terminals and mobile phones used for offline payments are insecure and can also be hacked. For the payment instruments, i.e. the cards, to trust instructions from intermediaries and for intermediaries to trust messages from payment instruments, digital certificates are used. In this case, the certificates were self-signed, but to achieve high security in a production-set solution, a trusted and verified PKI, *Public Key Infrastructure*, or equivalent, is required, to which issuance, signing and encryption can be linked.

In addition to digital certificates, payment instruments and e-krona engines use several different counters to ensure that offline payments are synchronised and that the instructions to and from the card have not already been processed. There is also protection against "*replay attack*", where the same e-krona is used multiple times. Each transaction also has a unique number that is stored in the intermediaries' e-krona engines.

3.3 Limits and restrictions

In an offline solution, it may be necessary to impose limits on the number and size of payments that can be accepted offline. The reasons may include reducing risks

and making money laundering and fraud more difficult. If restrictions are imposed, end users will have to go online more often to synchronise offline wallet transactions, which also helps intermediaries to see more easily which customers have money offline and how much. Once the synchronisation is complete, the card's counter is reset and new offline transactions can be made.

To evaluate how restrictions on the offline use of e-krona could be implemented, we introduced the following rules:

- Payment cards can carry out a maximum of five transactions offline.
- The balance on a card may never exceed SEK 3 000.
- A payment terminal can accept a maximum of twelve transactions offline.
- The amount of money received at a payment terminal may never exceed SEK 20 000.
- Money received by payment terminals in offline mode cannot be used for new offline payments.

The restrictions are implemented directly in the program code on the card and not as separate configurations. This made it easy to introduce the restrictions, but the disadvantage is that it can be difficult to change them afterwards if necessary.

Lessons learnt about limits and restrictions

It is entirely possible to impose restrictions on payment cards. Security features can be set on the cards, such as *write once,* and made permanent. The disadvantage is that you have to distribute new cards if you want to change the restrictions.

It can also be a bit of a challenge to explain to end users how limits and restrictions work in practice and how they might stop a payment in some cases. For example, a payer may have room left to make a payment offline, while the payment terminal is close to its limit for accepting the payment. This would mean that the payment could not be executed even though the payer is able to do so.

3.4 Transfers between online wallet and offline payment instruments

When users receive their card for offline payments, there is no money on the card. To use the card offline, the user needs to top up the card with money from the online wallet.

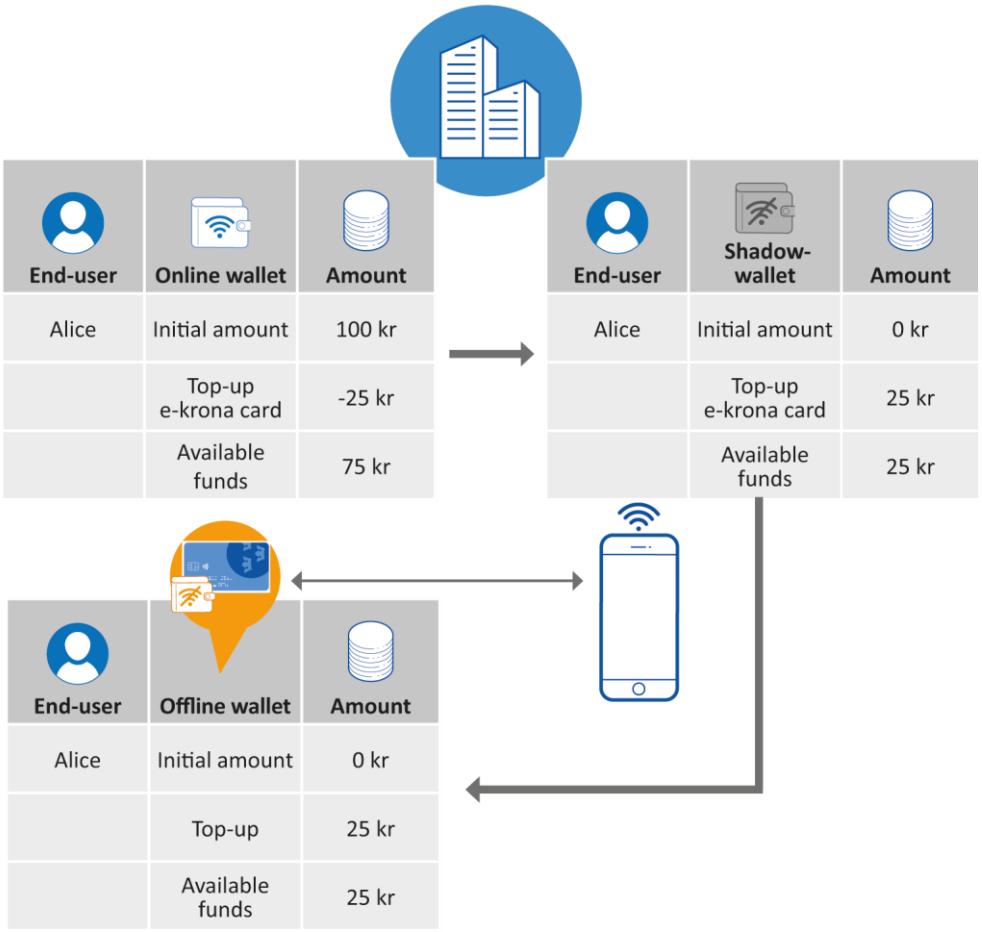


Figure 3. User charges their card for offline payments

1. Top up of payment cards is done as follows:
2. The user opens their e-krona app on their mobile phone and enters the amount to be transferred.
3. The user enters the PIN code of the e-krona app and brings the card to the NFC reader of the mobile phone.
4. The mobile phone creates a digitally signed request that is sent to the intermediary's e-krona node.
5. The intermediary verifies the digital signature and transfers the amount from the user's online wallet to the user's shadow wallet.
6. The intermediary reads the updated balance on the user's shadow wallet, signs the balance and sends the signed balance to the user's e-krona app.
7. The user holds the card against the mobile phone's NFC reader and the user's e-krona app transmits the updated balance to the card.
8. The card changes its balance to the updated balance value.

The user can also empty the card of any amount, see Figure 4. Before the card can be emptied, all offline transactions must be synchronised.

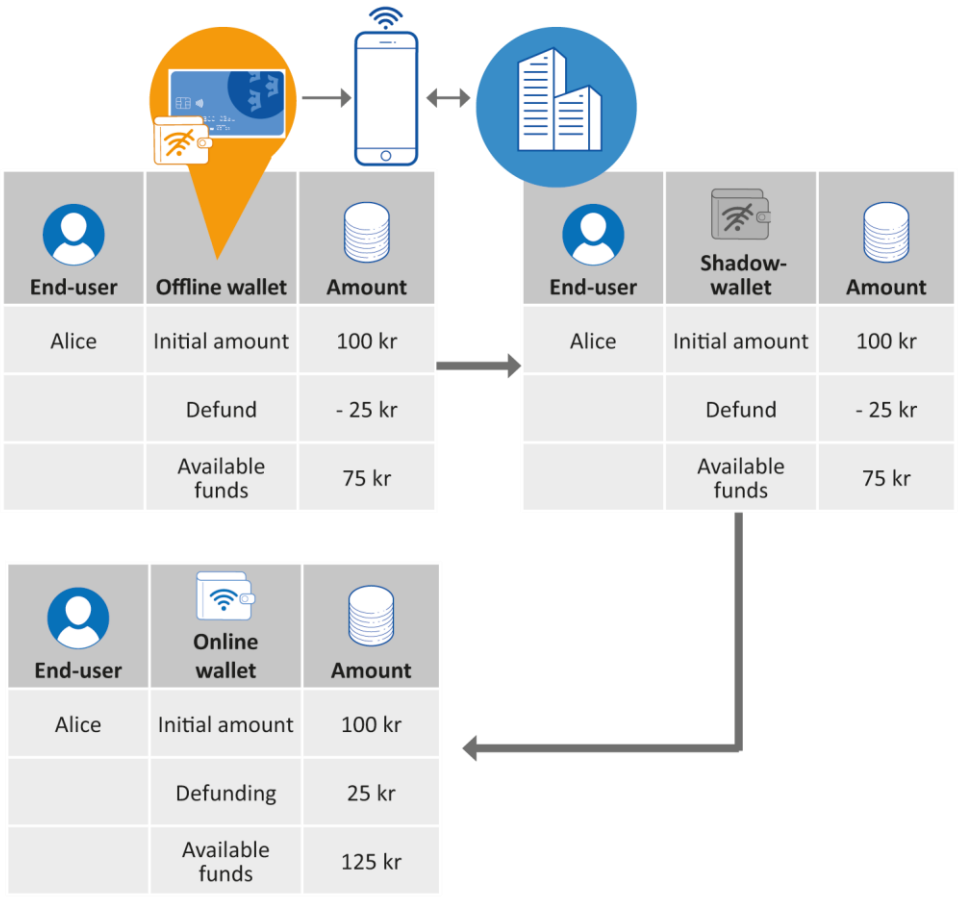


Figure 4. User reduces their amount for offline payments

Here's what an end user who wants to reduce their holdings of money that can be used offline should do:

1. The user opens their e-krona app on their mobile phone and enters the amount to be returned.
2. The user enters the card's pin code in the e-krona app and brings the card to the mobile phone's NFC reader.
3. The card verifies the PIN and transmits a one-time code to the e-krona app.
4. The e-krona app sends a request to the intermediary to return holdings. The intermediary verifies that the amount is in the user's shadow wallet.
5. The intermediary calculates what the future balance of the shadow wallet will be after the reduction and sends this balance value digitally signed back to the e-krona app.
6. The user holds the card against the mobile phone's NFC reader and the e-krona app transmits the signed balance to the card.
7. The card verifies the signature and updates the balance on the card.

8. The card sends back a confirmation to the e-krona app, digitally signed by the card, that the balance has been updated.
9. The e-krona app transmits this information to the intermediary.
10. The intermediary verifies the card's signature and transfers the amount from the user's shadow wallet to the online wallet.

Lessons learnt on transfers between online wallet and offline payment instruments

The intermediaries keep a shadow wallet for each user to distinguish which e-krona are available for offline transactions from those that can be used online. It is important for intermediaries to have information on the amount of e-krona in all offline wallets, both to manage risks and in the event that restrictions or fees are imposed on e-krona holdings. Each intermediary can calculate how many e-krona their customers have allocated for offline. However, it is important to emphasise that offline transactions between users at different intermediaries remain unknown until all outstanding offline transactions have been registered online.

One difficulty that needs to be addressed is the privacy of shadow wallets. The balance on the offline wallet, i.e. the offline payment instrument, is set by the intermediary's system. Therefore, there needs to be a control function to ensure that the balance recorded by the intermediary on the offline wallet reflects the balance on the shadow wallet. Otherwise, the intermediary could create money that does not exist in the online system.

3.5 Offline payments to merchants

We have also tested and evaluated how a user with an offline wallet can make offline payments to merchants. We used a solution for this that built on the *Point of Sale* payment terminal used in phase two. For the PoS terminal, an Android application was used that made it possible to use a regular Android phone as a Point of Sale terminal. The PoS terminal needs to be able to securely store offline transactions. However, the Riksbank was not able to use the secure storage and execution part of the mobile phone, the *Trusted Execution Environment*, and had to develop its own solution to protect payments from disclosure.

The data communication between payment card and PoS terminal used *Near Field Communication* (NFC).

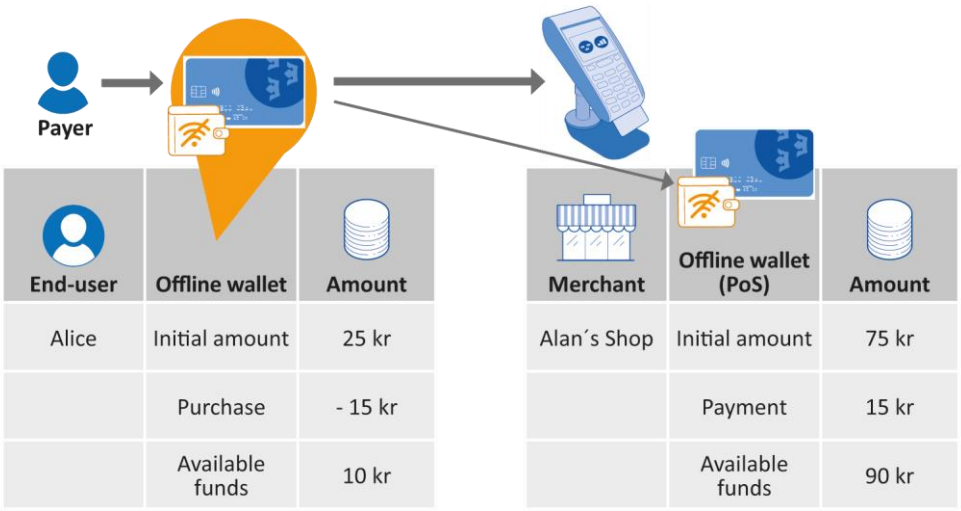


Figure 5. User makes an offline payment in store

The following steps are performed when a user makes an offline payment to a retailer's payment terminal:

1. The retailer starts the payment by creating a payment request, Request to Pay.
2. The PoS terminal displays the amount and prompts the customer to make a contactless payment with a PIN code.
3. The customer enters the payment card's PIN code and brings the payment card to the PoS terminal.
4. The card verifies the PIN, deducts the amount from the card balance and creates a digitally signed offline transaction containing the payer, recipient and amount.
5. In addition to saving the digitally signed offline transaction, the card also sends it to the PoS terminal.
6. The PoS terminal verifies the signature and saves the digitally signed offline transaction.
7. The PoS terminal displays a confirmation that the transaction has been received and registered.

The offline transactions stored in the PoS terminal cannot be tampered with without being detected during verification, as they are digitally signed. Without the private keys of offline wallets, they cannot be changed. It is also important to prevent outsiders from seeing the saved offline transactions. The PoS terminal, which is an Android app, creates its own encryption key and the offline transactions are encrypted before being saved. Key and encryption management in the PoS terminal is provided by Android's own KeyStore function.

Lessons learnt on in-store card payments

We can conclude that with a PoS terminal it is possible to accept payments offline with the limits we have used in phase four. The PoS terminal can store payment information encrypted, without having access to the secure storage and execution part of the mobile phone, the *Trusted Execution Environment*. However, we have

not fully verified the level of security needed to ensure that the transaction cannot be manipulated.

An important observation is that the payment is made in two separate steps. In the first step, the offline transaction is registered on the payer's card. In the second step, the payment terminal receives the offline transaction and only then is the transaction completed.

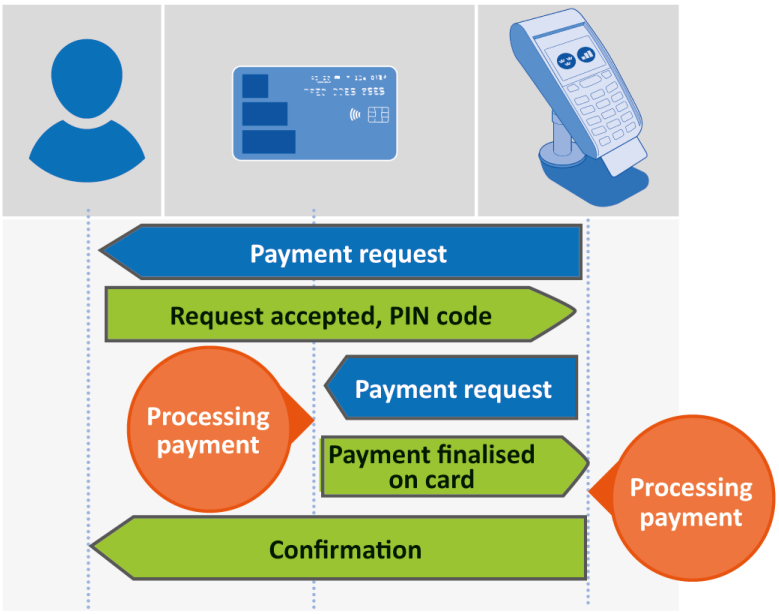


Figure 6. Payment from user to PoS terminal

However, there may be errors between the two steps, such as the card having executed the transaction and updated the balance but the PoS terminal not receiving a transaction or not processing it for some other reason. The result is that money has been deducted from the end user's card, but since the retailer cannot see it, the customer will not receive their goods. This is a problematic situation; the customer has "lost" money. If the customer were to synchronise their stored offline payments on the card, the retailer would get money deposited in their shadow wallet but the customer has not received anything for the money.

A solution that reduces the risk of such a situation was therefore implemented. A function was introduced that allows the last offline transaction on a card to be resubmitted if necessary. No new transaction is recorded on the card and the balance does not change, but the recipient is informed that the payment has been made.

It is important that each transaction is initiated by the recipient so that transfers cannot be made unless the recipient has requested it. The design is also such that all communication between the card and the PoS terminal can take place sequentially without having to "blip" the card several times, unlike the solution in phase two.

However, the PoS terminal does not sign payment requests which, if implemented, would increase security. If the recipient has signed a payment request, the card can verify the recipient and the transaction stored on the card is then

signed by both parties. It assures the payer that the recipient is who they claim to be.

In phase four, we used counters in the card to keep track of transactions made and synchronisations. We deliberately chose to implement counters as a security feature to prevent the manipulation of stored payments and to stop the possibility of repeating payments to create money, but the slightest error in these counters means that offline transactions and synchronisations are not carried out. An important unanswered question is also how existing PoS terminals need to be adjusted or replaced to accept offline e-krona payments.

3.6 Offline transactions between users

When a user wants to make an offline transaction to another user, a design that is user-friendly without compromising security is needed. We have used a payment card for secure storage and code execution of offline transactions. A mobile app is available for users to manage their card. The design chosen is similar to in-store card payments.

The objective was for the value to be transferred, in a highly secure manner, from the payer's offline wallet to the recipient's. The starting point for the design was that payers and recipients do not trust one another's mobile phones. The interaction and transaction would be through contactless transfer.

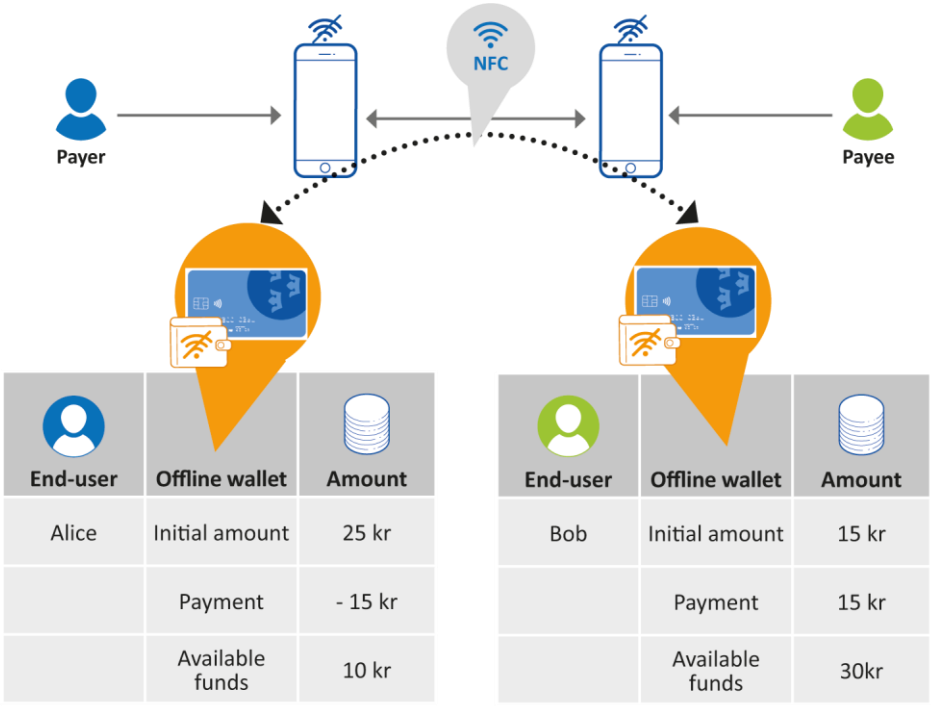


Figure 7. Offline transaction between two users

This is how an offline transaction between two users works:

1. The recipient selects an amount in their e-krona app and brings their card to their mobile phone. The card reads the amount and creates a digitally signed payment request that is sent back to the recipient's mobile phone.

2. The recipient and payer bring their mobile phones together and the signed payment request is sent to the payer's mobile phone.
3. The payer sees the payment request and authorises it by entering the card's PIN code and then swiping the card on the mobile phone. The mobile phone transmits the PIN and payment request signed by the recipient to the card. The card verifies the PIN, reduces its balance by the amount of the payment request and in turn signs the payment request and sends it back to the mobile phone.
4. The payer and recipient bring their mobile phones back together and the payment request, now signed by both cards, is transferred to the recipient.
5. The recipient accepts the payment by entering the PIN of his/her card and then swiping the card on the mobile phone. The mobile phone transmits the PIN and payment request to the card. The card verifies the PIN and signatures and then increases its balance by the amount of the payment request. The flow ends with the card reporting back to the recipient's mobile phone that the transaction was successful.

Lessons learnt about offline transactions between users

The secure design means that both payers and recipients have to go through many different steps and this reduces user-friendliness. In addition, both recipients and payers need to digitally prove ownership of their offline wallets via their respective signatures.

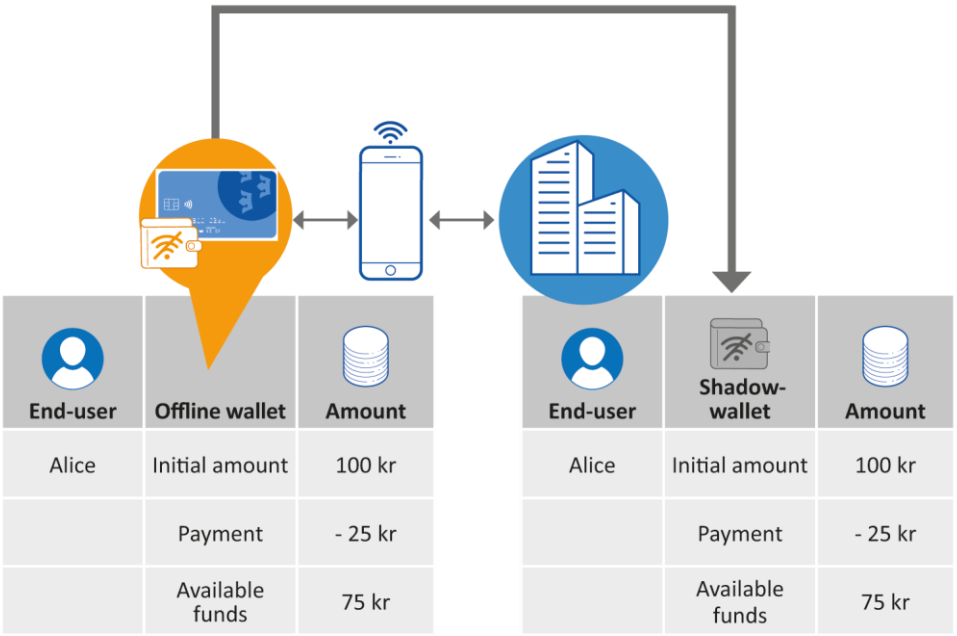
It must also be possible to process off-line transactions in cases where recipients choose to cancel and not receive an off-line transaction initiated by the recipient. In this solution, we have chosen to include various calculators in the software of the payment card that keep track of the transactions. Each initiated transaction is counted to prevent the same payment from being recorded twice. However, since we have set a limit of five offline transactions, more outstanding payments would simply stop further offline payments.

3.7 Synchronisation of saved offline transactions

If the PoS terminal or card has saved offline payments, they need to be synchronised. The idea of synchronisation is

- to be able to reset counters and authorise new offline transactions
- to read the current balance on the card
- to be able to record and settle offline transactions
- to be able to identify anomalies such as double spending or money creation.

The flows for cards and PoS are very similar but differ in some respects.



End-user	Offline wallet	Amount
Alice	Initial amount	100 kr
	Payment	- 25 kr
	Available funds	75 kr

End-user	Shadow-wallet	Amount
Alice	Initial amount	100 kr
	Payment	- 25 kr
	Available funds	75 kr

Figure 8. Registration of outstanding offline transactions (synchronisation)

Synchronisation of offline transactions needs to be carried out in several steps. One model is to allow the synchronisation to start automatically every time the user checks the card's balance when the mobile phone is online. But to make it easy to test the solution, we chose a design where the end user manually initiates a synchronisation:

1. The end user chooses to manage their card in their e-krona app, enters the card's PIN code and then brings the card to the mobile phone.
2. The PIN code is transferred to the card that verifies it. If the card has saved offline transactions, they are sent to the mobile phone. For the PoS terminal, the app can read the transactions directly from the database.
3. The mobile phone forwards the transactions to the intermediary.
4. The intermediary verifies the transactions. The intermediary executes any transaction not previously known to it by moving e-krona from the payer's shadow wallet to the recipient's shadow wallet.
5. The intermediary reads the updated balance on the user's shadow wallet, signs the balance value and sends it to the user's e-krona app.

6. The user holds the card against the mobile phone's NFC reader and the user's e-krona app transmits the updated balance to the card.
7. The card changes its balance to the updated balance value and resets the offline transaction counter to zero and deletes saved offline transactions.

Settlement of offline payments

Payments between payers and recipients in the offline solution are not finally settled until they are synchronised with the shadow wallets in the online system. All offline transactions are always recorded in both payment instruments. This means that settlement takes place when the first payment instrument synchronises. When the other payment instrument synchronises, a check is made whether the current transaction has already been settled. If so, no further action is taken. This is so that a payment is not duplicated when both the payer and the recipient synchronise their offline payments.

When the payer and recipient are with the same intermediary, the transfer can be performed directly between the two shadow wallets regardless of who synchronises first. If the payer and the recipient are with different intermediaries, in some cases a request for payment needs to be sent between intermediaries as follows:

If it is the PoS terminal that is synchronised, the intermediary needs to make a request for payment from the payer's shadow wallet to the merchant's shadow wallet. If it is a card that is synchronised, there is a check of whether the offline payment is from or to the card. If it is to the card, it works the same way as for the PoS terminal and if the payment is from the card, the intermediary performs a regular transfer from the card's shadow wallet to the recipient's shadow wallet.

To request a payment, the recipient's intermediary sends the transfer request to the payer's intermediary, which sends the requested amount without verification. The whole flow is highly simplified in the e-krona pilot and for it to work in reality, the e-krona engines of the different intermediaries need to be able to send messages to one another.

When all offline payments are synchronised, the intermediary sends back a signed reset message so that the card or PoS terminal knows that the transactions have been synchronised and that any restrictions can be reset.

Lessons learned on synchronising stored offline transactions

Implementing synchronisation means

- reading saved offline transactions and updating the e-krona network's shadow wallets.
- resetting the card's transaction counter so that new offline transactions can be carried out.
- updating the card's balance to reflect the updated balance of the shadow wallet.

Communication errors can occur at several points, as synchronisation is entirely dependent on a mobile phone transmitting information between the card and the

intermediary. This may mean that the update takes place in one place but not in another, for example the shadow wallet is updated but not the payment card.

During the design process, there was discussion of the possibility of introducing feedback from the offline wallet to the intermediary to ensure that the update is completed. However, this would not help if the communication was broken in the final step, because the intermediary would have to deal with this situation instead.

Other problems that may arise during synchronisation are the following:

- The card is not synchronised and therefore the transaction counter is not reset to allow new offline transactions.
- The counters on the card and the corresponding counters at the intermediary differ in a way that is not expected. This puts the card in an unusable state.
- An offline transaction on the card is rejected by the intermediary.

Some of the problems could be solved by re-synchronising the card or by topping up the card with more money. Then the balance and the counter would be updated.

Liquidity problems in synchronisation

During the analysis and design of the solution, we discovered that a situation may arise where there is a lack of funds in a payer's shadow wallet.

This situation arises when several users make consecutive transactions and no one goes online.

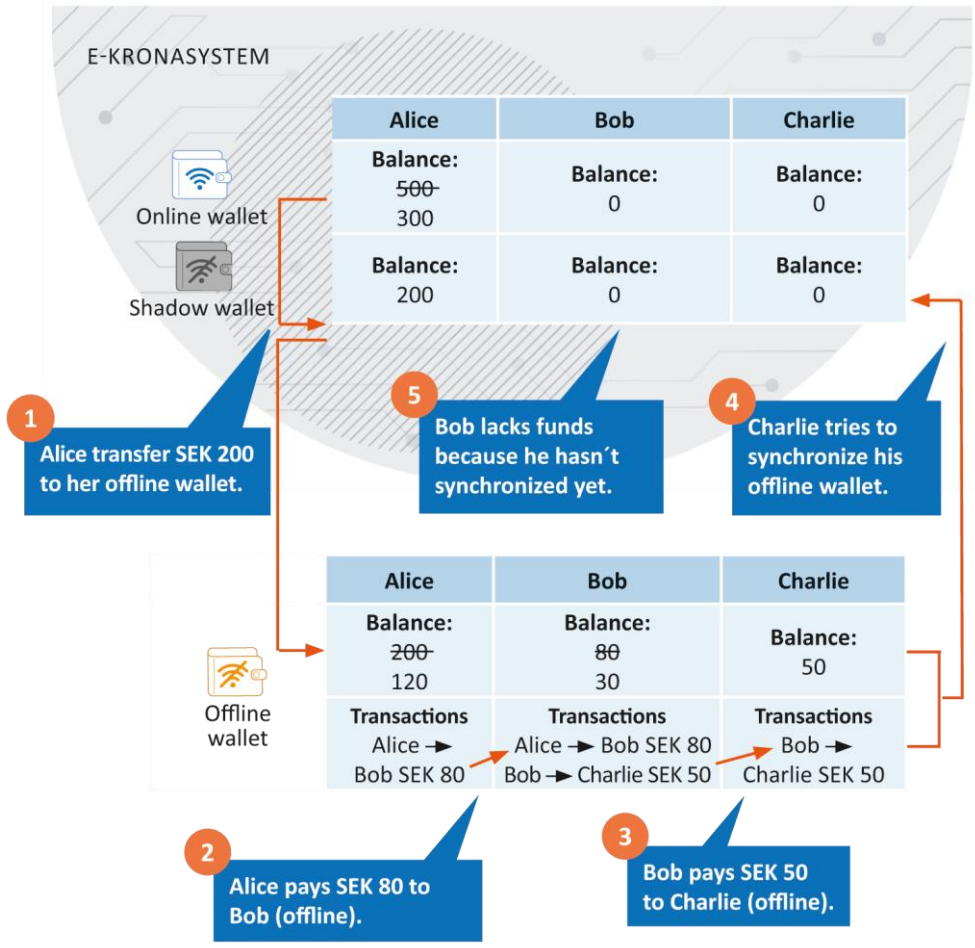


Figure 9. Liquidity problems in synchronisation

Example: Alice transfers SEK 200 to her offline wallet (1) and thus has a balance of SEK 200 in her shadow wallet as well. In offline mode, Alice pays SEK 80 to Bob (2) who in turn pays SEK 50 to Charlie (3). Now Alice has SEK 120 in her offline wallet, while Bob has SEK 30 and Charlie has SEK 50. Alice's shadow wallet still contains 200 SEK, while Bob's and Charlie's are empty because no synchronisation has been done yet. If Charlie goes online to synchronise (4), a problem arises as the SEK 50 that Charlie has received from Bob cannot be moved from Bob's shadow wallet (5) as the balance there is 0. However, if Alice or Bob has synchronised before Charlie, there will be funds for the transaction.

The Riksbank has investigated how to solve this problem. One possibility is for the central bank to provide a liquidity pool for the payments, another is to impose restrictions on how money can be used offline, e.g. money received in offline mode cannot be used for offline payments until the payment instrument is synchronised. However, the Riksbank has not made any in-depth analyses of these possible solutions and therefore cannot say what is feasible.

3.8 Lessons learned on security design

During this phase, a number of insights have emerged that would need to be further explored and addressed. A selection is given below:

- Instructions and payments to cards are not uniquely addressed which becomes a security issue. Because of this, for example, loading the cards can be replayed in a so-called replay attack.
- An offline payment could be executed twice if the payer and recipient synchronised at exactly the same time. In this so-called *race condition*, both intermediaries search their databases for the transaction number at the same time and both execute the transfer because neither finds the transaction.
- Instructions to the cards are not signed by the intermediary, which is a theoretical weakness. For example, another party could programme a card to carry out other instructions.
- A recipient should be able to choose not to receive a payment. Due to the design, this is not possible. If the payer has initiated the payment, it is already registered on the payer's card and will therefore be executed when the payer synchronises this payment.
- The limits implemented on payment cards, such as maximum balance and number of offline payments, are hard-coded and cannot be changed without distributing new cards.
- The PoS terminal's private key for offline payments is not fully protected. The PoS app could be manipulated to sign any message. This flaw could be exploited for various types of fraudulent payment.
- There are different counters on the offline cards and matching counters at the intermediaries. It is a simple and effective solution to maintain the integrity of the solution. However, the different counters can become out of sync, for example if a card fails to record a message. It is then not known whether the errors in the counters were caused by attempted attacks or technical bugs. It is a challenge to deal with different types of error without jeopardising the integrity of the system or the user's money.

SVERIGES RIKSBANK
Tel. +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK
ISSN ISSN. (on-line)