E-krona report

E-krona pilot Phase 2

April 2022

SVERIGES RIKSBANK

1 Table of contents

Summary

In February 2021, the second phase of the e-krona pilot began. The aim of the work was to continue developing and testing the technical solution on which the e-krona pilot is based, and also to investigate a potential legal framework around the e-krona. Phase 2 has been instructive and has given the Riksbank deeper knowledge in preparation for the continued work on a potential e-krona. This report aims to summarise the work carried out during this phase and the conclusions drawn and lessons learned by the Riksbank.

Integration of participants

The focus of the work has been on testing how the network for distribution and use of the e-krona (hereinafter referred to as the e-krona network) established in a test environment during Phase 1 could be integrated at potential distributors and with the existing payment infrastructure. [1] The work carried out together with Handelsbanken and Tietoevry as participants in the e-krona network has meant that we have tested the solution where e-kronor issued by the Riksbank are distributed to end-users via the participants. The end-users could then hold and use e-kronor in transactions on an e-krona network that exists parallel to, but integrated with the participants' internal systems and the payment infrastructure. The work has also shown how a DLT and token-based solution on the Corda platform enables a parallel e-krona network that clearly differentiates between privately-issued money (account balances) and the e-krona that would be issued and guaranteed by the state. [2]

Alias for addressing

Phase 2 has also investigated and implemented a more user-friendly way of addressing transactions in the e-krona network. An alias service allows each wallet's technical address to be connected to a more user-friendly alias. The alias service is centralised and end-users can invoke the service through their participants. A centralised solution provides an effective means of creating, storing and using aliases within the network, but it also raises a number of questions as to how it will work together with the concept of a distributed model aimed at minimising dependence on centralised parts.

[1] For more information on the solution tested and the work done during Phase 1, please see: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf

[2] DLT (for *Distributed Ledger Technology)* and tokens have no clear definition. DLT means in the pilot solution that the transactions are not recorded in a central database, but in the nodes of the participants directly involved in the transaction. The tokens in the pilot's solution can be described as uniquely identifiable digital value units with the property of being able to represent e-kronor. In the e-krona pilot, so-called fungible tokens are used, which can be divided and combined into new tokens that represent a smaller or larger amount of e-kronor.

One important question, if a centralised solution is chosen, will be where the responsibility for the alias service will lie. It is likely that the responsibility could fall to the Riksbank as owner of the e-krona network, and if so, further investigation would be needed into what this entails. Other simple addressing solutions such as QR codes are becoming more common and could be of interest for an e-krona, too. However, these have not been technically investigated in the pilot.

Wallet models and opportunities for off-line payments

The work in Phase 2 has also demonstrated how the token-based solution can be used in different ways to store e-kronor. This makes it possible to design different wallet types for different purposes. One type means that tokens are stored at the network participant. The design provides an e-krona that for end-users is similar to the way digital money in accounts works, even though the underlying technology differs from account-based systems. This makes it possible to offer the same kind of services and user experiences that we are used to today, for example multiple payment instruments that are connected to the same money and other payment services, such as direct debit. The second wallet type is based on end-users storing e-kronor in a local wallet on their mobile phone. This allows transactions to be made off-line. However, such transactions would not be settled, which entails certain risks. It has also been shown that it is not always possible to get back locally stored e-kronor if you lose your wallet. Therefore, locally stored e-kronor should be considered as cash, and only held in limited amounts for use off-line. While it would be technically possible to minimise the risks, there are other risks associated with off-line transactions, such as money laundering and criminal activity, which may require restrictions.

Integration with POS terminal

Phase 2 has also tested the integration of the e-krona network into a POS terminal (point of sale) that is present on the market today. This has shown that it is possible to install e-krona specific software on a terminal to enable payments to be made within the e-krona network, at the same time as the terminal can handle payments on the large card networks. The major questions here are not necessarily technical, but rather what policy objectives and regulations should apply to an e-krona, for example, how independent and parallel an e-krona should be in relation to other parts of the payment infrastructure. Integrating the e-krona into the existing terminal market is a complex issue, which often involves adjustments to regulations and to the terminals of private operators. Developments in the payment market, both in Sweden and abroad, show that app-based payments and new types of mobile terminals are becoming increasingly common. It will be important to monitor the continuing developments and ensure that an e-krona and its regulatory framework are flexible and able to function in such payments.

Performance tests

Another important focus area for Phase 2 has been to continue testing the performance of the technical solution. A fundamental requirement for the e-krona is that it should enable instant transactions on a large scale and that this should be possible 24/7, 365 days a year. The work has included a comparison with the transaction volumes of Swish and a card network during their most busy times of year. The fact that the tested solution is token-based and DLT-based means that it has certain properties that can pose challenges with regard to performance. To test the solution and understand where problems might arise, we have designed scenarios to see where possible bottlenecks could be created. The tests have shown that, in the simpler scenarios, the solution corresponds well to the same transaction volumes of Swish and a card network. As transactions become more complex with more tokens and longer historical transaction chains, performance is reduced. Suggestions for technical measures to resolve these issues have been discussed, but they are so far untested and further work would be required to test and evaluate the impact of these measures on the performance and solution as a whole.

Legal questions

Work in the legal field has mainly focused on two areas: how information is shared in a DLT network and how the legislation would be applied to such information sharing when it comes to financial confidentiality and data protection, and also on the question of what type of asset the e-krona would be.

The legal analysis shows that it is not clear how the sharing of information that DLT/block chain technology is based on relates to current legislation with regard to financial confidentiality and data protection. It is likely that the data accompanying a transaction in the transaction history will be considered personal data and subject to financial secrecy. Legal changes and/or information security measures may be required if the solution tested in the pilot is to comply with applicable law.

According to the legal analysis, the e-krona in the pilot may be regarded as an electronic form of the asset class cash. It will then be a new alternative and complement to the physical form of cash that is available today – banknotes and coins.

Conclusions

To summarise, Phase 2 has focused on continued testing of the technical solution and digging deeper into the more complex issues of a potential e-krona. The work has shown how a parallel network with e-kronor, like the tested solution, could be integrated with participants' internal systems and enable the distribution of, and transactions with, e-kronor. It has also shown how the token-based solution can design wallets similar to a regular account for the end user, but also wallets whose e-kronor in some respects have more cash-like properties. By testing the integration of the e-krona network with a POS terminal, it has been demonstrated in practical terms how the network could use existing hardware used in the market today to handle card network payments. The work has also highlighted the importance of regulatory framework and cooperation models with the payment market players if an e-krona is to be established in the retail trade. Phase 2 has also made it clear that the tested Corda platform is not specifically designed for a so-called retail CBDC that the e-krona would be (the platform is essentially designed for other types of financial transactions). It has, for instance, become clear during the work on performance tests where the scenarios that an e-krona must manage may entail problems in the current version of the Corda platform. This also applies to sharing data within the network, which is a basic idea of DLT technology, but raises questions about whether the platform can meet the requirements in the legal regulations. The technical adjustments needed to address these potential problems, such as automated redemption of e-kronor with long transaction chains, are untested and at the same time raise other questions. The challenges that the platform has do not mean that this type of solution needs to be inappropriate for a potential e-krona. However, it requires that the weaknesses identified can be addressed in future releases and in the design of an e-krona network.

An e-krona, regardless of design and technology, will mean that the public has access to a new form of money issued by the Riksbank. The different issues relating to an e-krona are often complex, some from a purely technical perspective, others from a policy perspective and others with regard to how responsibilities and roles should function in a distribution model for the e-krona. Add to this the legal issues that need to be resolved with regard to a new form of money. During Phase 2, many of these issues have been addressed and for the pilot project's purpose of increasing the Riksbank's knowledge, the work has been valuable. This provides a good basis for the Riksbank's continued work on the design and requirements for a possible issuable e-krona.

The Riksbank would like to pay special thanks to Handelsbanken and Tietoevry, who contributed to the Riksbank's learning process by participating in Phase 2 of the e-krona pilot project.[3]

[3] Handelsbanken is one of the major banks in Sweden and Tietoevry is a major supplier of IT systems for banking services, among other things.

1 Background – cash use constantly declining

Banknotes and coins are increasingly rarely used in Sweden. This is partly due to technological advances, which have given us different types of modern digital payment services. However, the Riksbank sees potential problems in the fact that the money issued by the Riksbank and available to the general public is on the verge of disappearing. Since 2017, the Riksbank has therefore been examining the possibility of developing a digital alternative in central bank issued money, a so-called e-krona.

In February 2020, the Riksbank initiated a more practical stage of the work on an e-krona through a technical pilot project together with Accenture, in which a possible solution for an e-krona has been tested. During the first phase of the e-krona pilot, an e-krona network was created on a platform based on *Distributed Ledger Technology* (DLT), where the e-krona was represented by tokens. In February 2021, the work moved into the second phase, which involved further investigation and testing of the technical solution's potential to meet the possible requirements of an issuable e-krona.

There is still no decision to launch an e-krona, nor as to what technology would then be used or what the legal framework would be like. The purpose of the pilot is for the Riksbank to learn more, through practical work, about how an e-krona might work. The work should be regarded as a way for the Riksbank to obtain a better basis for comparisons with other possible solutions and as a way of investigating both technical and legal details. The solution developed within the pilot is thus not intended for production.

2 Technical work Phase 2

An e-krona will need to be compatible with existing market players and payment infrastructure so that it can be distributed to the public and used in transactions. The technical work during Phase 2 has therefore focused on testing how these integrations would work and how the e-krona could be used as a means of payment in different situations. We have also tested whether the technical solution could be used for instant mass payments. The work has shown that the technical solution can be integrated with existing infrastructure and also that it is flexible to design solutions for various payment services and situations. The fact that the solution has so far not been used in production for a retail CBDC has, however, highlighted some of its performance challenges.

2.1 Successful integration of participants

One focus area for Phase 2 of the e-krona pilot has been to test how the developed e-krona network could be integrated with the internal systems of potential participants. This is a basic prerequisite for the model on which the solution is based, where the Riksbank creates the e-kronor and where distribution to the public takes place via approved participants in the e-krona network. Handelsbanken and Tietoevry have participated in Phase 2 of the e-krona pilot, in the role of bank and supplier of financial IT systems, where they have operated a node in the e-krona network and integrated it with their existing account and payment systems. It has thus been possible to see how a potential participant in an e-krona network could order e-kronor from the Riksbank and offer its customers the possibility to exchange e-kronor for account credits in the account system. The integration work has shown that the tested solution can be used to create a parallel network, where e-kronor issued and guaranteed by the Riksbank exist. We have also tested making transactions between participants and end-users within the e-krona network and also outside of the e-krona network.

Distribution model similar to current model for cash

The technical solution tested in the e-krona pilot is based on a so-called two-tier model where the e-kronor, like the model with physical cash, are distributed from the Riksbank to the general public via approved participants in an e-krona network. The participants may be banks or payment service providers, for example. The e-krona network is based on the R3 Corda platform, which is based on DLT, and the e-kronor in the network are represented by tokens that can be traced back to the Riksbank as issuer. The participants in the network operate nodes and can order e-kronor from the Riksbank which are debited from their reserves in the Riksbank's settlement system, RIX. The participants can then store the e-kronor in their digital vaults. Participants offer their customers as end-users the possibility to open digital e-krona wallets that can be linked to payment instruments, such as mobile apps or cards.[4] The e-krona wallet is also linked to the customers' accounts in the participant's internal system, where the customers have their account credits.[5] This allows end-users to exchange e-kronor from the participant's vault and pay for them with their account balances with the participant. And the opposite is true if customers want to exchange e-kronor for account credits. End-users can then make transactions with the e-kronor through their connected participant's nodes on the network. It is important in this distribution model that end-users connect to the e-krona via already established customer relations with the participant distributing the e-krona. It is therefore assumed that the end-users are already customers of the bank or payment service provider, have accounts there and are known as customers (KYC). The Riksbank, as issuer of the e-krona, is therefore not responsible for the connection of customers, or for the processes surrounding this.

Integration with focus on exchange and transactions

The solution is thus based on the participant's node in the e-krona network being integrated with the participant's internal customer, account and payment systems. This allows a connected customer to open a wallet and link it to an account and exchange between account credits and e-kronor. Integration with other internal systems of the participants, such as accounting systems and AML systems, is also necessary for a production solution, but this has not been tested during Phase 2. Handelsbanken and Tietoevry, as pilot participants, have each run a node in the e-krona network and this has been linked to the participant's internal banking system through an integration layer (described in more detail below).

[4] In the e-krona pilot a mobile app has been developed on phones with Android OS, and a card has also been tested as payment instrument during the work.

[5] During Phase 1, the possibility of having so-called anonymous wallets that do not require identification or connection with a specified account with a participant was also tested. This type of wallet would probably have limits on the amount allowed and on the ability to receive transactions and could, for example, be purchased at authorised retailers.

FACT BOX – integration via *an e-krona engine*

Corda, which is the DLT platform on which the e-krona network is built, is not specifically designed for the so-called *retail CBDC* which the e-krona would be. The platform has a broader, more general, area of use for transferring digital assets in the form of tokens within a distributed network. To use the platform for an e-krona, an integration layer is needed, in the pilot called the e-krona engine. The e-krona engine can be described as a business and integration layer that allows the e-krona network to be connected to a participant's internal system and structures the information from the DLT network in a way that users understand.

To give an example: As mentioned above, the e-krona is represented in this technical solution by individual tokens whose value in e-kronor may vary.[6] For an end-user, e-kronor can consist of a variety of tokens with different values, in the same way that you can own a variety of physical banknotes and coins. But for an end-user, the individual tokens that build up your total ownership of e-kronor are uninteresting. What is of interest is how much e-kronor you have. The e-krona engine enables integration with the participants' internal systems and simplifies and compiles information from the Corda platform. For example, it sums up each end-user's balance, enables the display of transaction history, manages aliases and other necessary services that allow the Corda platform to be used for the purposes of an e-krona.

At this stage of the pilot, the focus of the integration has been mainly on the account and payment system to test the basic functions. The integration work with the participants has resulted in Handelsbanken and Tietoevry being able to

- request the issue of e-kronor from the Riksbank, against a debit of their reserves in a simulation of RIX, and to store these in their e-krona vault
- open e-krona wallets for their customers and link their wallets to payment instruments and payment accounts with account credits
- allow customers to exchange e-kronor for account credits
- allow customers to make transactions with e-kronor to other e-krona wallets within the network
- allow customers to carry out transactions with e-kronor to payment accounts at the participant (which means exchanging with the participant who receives the e-kronor and credits the commercial payment account)
- allow customers to exchange e-kronor for account credits
- request redemption of e-kronor at the Riksbank against crediting reserves in a simulation of RIX.

[6] The technical solution is based on asymmetric cryptography, where each token with e-kronor is also linked to a key pair. A public key that is open and shows who is the owner of the token. A private key that is tied to the owner of the e-kronor, who can thus carry out transactions with tokens using the matching public key. This connection of public key and e-krona wallet, which in turn is linked to a specific customer, is also made in the e-krona engine. The keys are held by the participant and not apparent to the end-users.

During the pilot, the participants have chosen different ways of implementing and carrying out tests of these flows. Handelsbanken developed its own web-based test interface solely for the purpose of the pilot. Partly to be able to control the bank's own orders and redemption of e-kronor from the Riksbank, and partly to simulate how their customers could make exchanges and transactions.

Tietoevry built a web interface for the pilot to demonstrate how a banking system could order and redeem e-kronor and keep a book of its e-krona holdings. They also developed a tool that could automatically request issuance or redemption at the Riksbank as soon as the proceeds in the vault were below or above certain limits. To simulate end-customer exchanges and transactions, Tietoevry used the app developed during Phase 1 of the e-krona pilot and a web interface it developed itself. [7]

Handelsbanken and Tietoevry's own implementations and tests have demonstrated how participants could operate nodes in the e-krona network with linked integration layers and develop their own interfaces and administrative tools to implement their own business rules adapted to their own operations and their customers. The participants' connection to the Riksbank's e-krona network was also implemented in various ways. For one participant we chose to move the e-krona into their own internal IT environment. In the second case, we chose to leave the e-krona node in the environment that the Riksbank set up for the e-krona network. Figure 1 illustrates how the e-krona network was set up. Tietoevry's and the Riksbank's nodes were implemented in the same IT environment as set up for the pilot, while Handelsbanken's node was located in their own IT environment. But all parties were able to communicate and carry out transactions on a common e-krona network.[8]

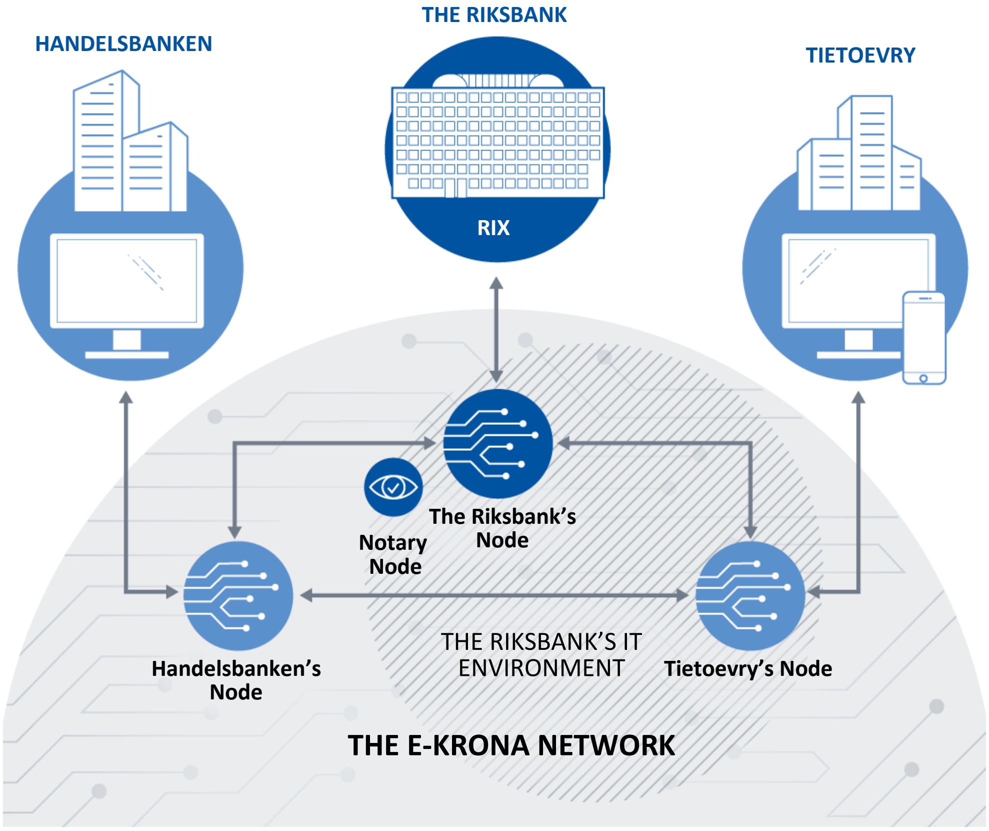
One lesson learnt from this design is that two participants can integrate with the system in different environments and when they are later merged into one environment, no further testing is required for them to interact.

[7] Under the headinghttps://www.riksbank.se/sv/press-och-publicerat/konferenser/2021/2021-11-29/ there are demonstration films from Handelsbanken and Tietoevry's implementations and proprietary interfaces from Phase 2.

[8] The communication between the Riksbank and the participants in the network has in the pilot gone over the Internet through VPN. For a production network, there would be higher safety requirements on the communication routes, but for the pilot's purpose this has worked well.

Figure 1. This is how the participants have been integrated into the e-krona network

The figure illustrates how the participants' e-krona node in the network is integrated with their internal account systems and payment systems. Handelsbanken has implemented its e-krona node in its own IT environment, while Tietoevry's e-krona node is in the Riksbank's IT environment.



Lessons learned from the integration activity

The work on integrating external actors as participants has made the concept of an e-krona system and a network where digital central bank money circulates concrete. The e-kronor in this network are issued and guaranteed by the Riksbank, although they are distributed to the general public via participants in the network. The fact that the e-kronor are represented by uniquely identifiable tokens in their own network makes them clearly distinguishable from other digital money in the form of account credits to which the public has access today. The work has also shown how a parallel network integrated with existing account and payment infrastructures can function. The parallel operation of the network can make the payment market more robust and the integration with existing account and payment infrastructures will enable direct exchanges and transfers between account credits and e-kronor. The network is therefore dependent on the functioning of the adjacent account and payment systems to make it possible to replenish liquidity in the wallets, but is in parallel in that transactions *within* the e-krona network are not strictly dependent on the adjacent systems. The work with the participants has also shown that for players such as Handelsbanken and Tietoevry it need not be a major technical challenge to integrate an e-krona network, like the one tested in the pilot, with internal banking systems, as long as one follows industry practice. This has also been emphasised by the participants themselves, who are used to working with the integration of different systems. However, what was tested in the pilot was only part of the integrations and safety requirements that would be required for production. The regulatory framework that would apply to an e-krona would of course also determine how integration with the participants would need to work. However, such policy issues have not been in focus during this stage of the pilot.

2.2 Alias for addressing

The Swedish payment market is currently at the forefront in terms of user-friendly instant digital payments. This is also an explanation of why physical cash is used less and less frequently. The possibility to address transactions in a user-friendly way is therefore a prerequisite for whether an e-krona can be established and used. The DLT platform on which the e-krona network is based has no built-in solution for this, so one focus area for Phase 2 of the e-krona pilot was to investigate how this could work in a distributed network and implement a technical solution for it.

As mentioned above, the Corda platform on which the pilot's technical solution is based is not designed specifically for the purposes of an e-krona. For example, the platform provides only a technical address for the wallets, whose ID consists of a long complex alphanumeric string.[9] Therefore, a solution is needed that links the wallet ID to something that is easier to address. For example, the payment app Swish has solved this so that you can address a bank account via a mobile phone number, which is much easier than using the underlying account number. The solution we chose to test in the pilot became a standalone central component of the network that enables end-users to create and store their own aliases for their wallets, making it easier to address transactions.

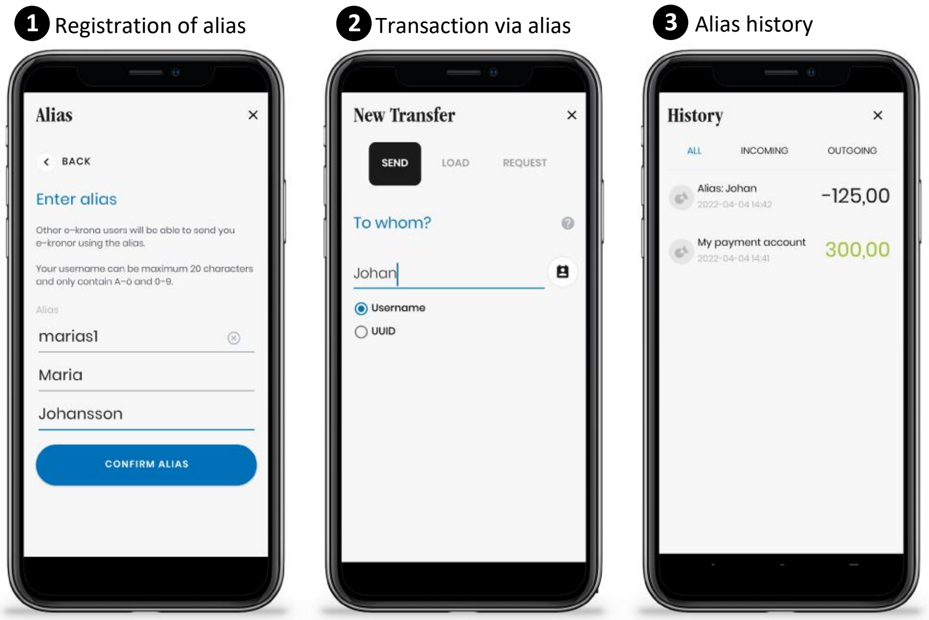
Implemented alias service

The ability to create an alias implemented during Phase 2 allows the end-user to tie their wallet and its ID to an alias via the interface of the mobile app developed for the pilot. We have here assumed that it will be possible to use any name as an alias. This is because one user could have multiple e-krona wallets. The work has not focused on whether or not this was the best thing for production. For this alias service to work with other addressing solutions, there may also be good reason to comply with certain standards. But technically, there is nothing to prevent the introduction of greater restrictions as to what an alias might look like. But for the purpose of the pilot, with the tests that have been carried out, a freer naming process has been preferable. Figure 2 shows examples from the implemented interface of the pilot's e-krona app.

[9] The alphanumeric string is a 30-character ID (in the Corda UUID for *Universally Unique Identifiers*) consisting of letters and numbers.

Figure 2. Interface when using alias

Example images from the pilot-developed test app on how the implemented alias service works when registering aliases, and the use of aliases in transactions.



1 Registration of alias

Alias

Enter alias

Other e-krona users will be able to send you e-kronor using the alias.

Your username can be maximum 20 characters and only contain A–ö and 0–9.

Alias: marias1

Maria

Johansson

2 Transaction via alias

New Transfer

To whom?

Johan

● Username

○ UUID

3 Alias history

History

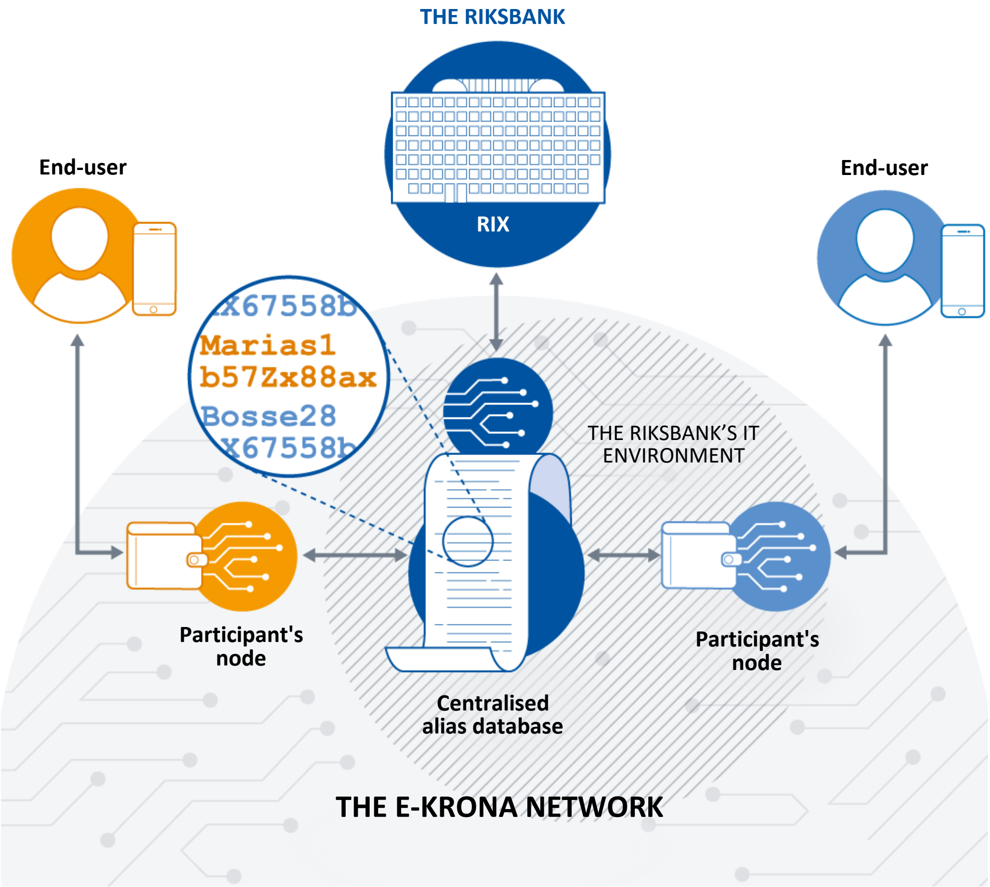
Alias: Johan 2022-04-04 14:42 -125,00

My payment account 2022-04-04 14:41 300,00

However, the most important thing in Phase 2 was not to examine how it would look graphically in the app developed solely for pilot testing purposes, or to determine what limitations would apply in the selection of aliases. It was more interesting to understand how a DLT platform, which is basically not designed for the kind of addressing that an e-krona needs, can build an alias service effectively. The alias service developed in the pilot is designed as a separate central component of the network with which participants' e-krona nodes can communicate. When an end-user enters an alias, it is done via the participant’s e-krona engine, which calls the network’s central alias service that stores the specified alias together with the associated wallet ID. And when a payment is to be made to that wallet, the alias can be used for addressing. Technically, this means that the paying participant calls the alias service to find the associated wallet ID that the platform uses to send the payment using the alias. An alias thus becomes a way to retrieve the underlying wallet ID through a central component. The loose connection of the alias service to the other parts of the e-krona network mean that the alias service can be changed or replaced if the network were to be connected to other established addressing standards. This can be done without affecting the other functions of the e-krona engine. Figure 3 shows a simplified illustration of how the alias service works.

Figure 3. How the alias service has been integrated into the e-krona network

The alias service is a central component of the network that participants' nodes can call when making payments using aliases. The end-user alias is connected to the technical addressing that exists on the network



Lessons and reflections from work with aliases

An important issue for further investigation is what it means for the concept of a distributed network if more centralised components such as the alias service are introduced. A possible disadvantage of a centralised alias service is that the network thereby becomes dependent on a centrally stored service to use aliases.

This weakness can be remedied by allowing other ways of addressing within the network. In Phase 2, one could also use the app produced for the more complicated wallet ID for addressing if the alias was missing, or if there was a service disruption. It is also technically possible to design a more decentralised solution for an alias service, which has been discussed during the pilot's work. However, this becomes much more complex and involves other kinds of dependencies on communication between participants when, for example, updating an end-user's alias. Another important issue if you use a centralised alias service is who is responsible for developing and managing data. It is likely that the responsibility could fall to the Riksbank as owner of the e-krona network, even if it was outsourced to an actor outside the Riksbank's IT environment. This could mean that the Riksbank would be given responsibility for the user data in the e-krona network, which the Riksbank, using this model, wishes to avoid to maintain its current role in the payment market and not need to handle data on end-customers.

QR codes are another tried and simple way of addressing that is becoming increasingly common in the retail trade and is also very common in some countries, such as China. Such a solution could be interesting as an alternative to an alias service, since it is absolutely essential that payments with an e-krona can be addressed in a user-friendly way. However, the information about who is associated with a specific QR code will be needed just the same as with an alias. Before you can build an address service, for example via aliases, on a technical solution that does not have built-in support for it from the beginning, a number of questions have to be answered. These include both technical questions about how to make it as user-friendly as possible and questions about where the information should lie and who should have ultimate responsibility for it.

2.3 Wallet models and opportunities for off-line payments

An important area for the e-krona pilot is to investigate how a potential e-krona could offer opportunities for making payments off-line, that is, without communication links to an e-krona network. As cash is becoming increasingly marginalised, the risk of the payment market, and thus the Swedish economy, becoming increasingly vulnerable to disturbances or problems with existing digital payments is increasing. The possibility of being able to pay off-line is therefore of great interest to a potential e-krona, and it is also highlighted in the general CBDC debate.

The work in Phase 2 has shown that it is possible to store the e-kronor locally on a mobile phone. This makes off-line transactions possible, but since the solution is based on an on-line e-krona network, off-line transactions pose risks that would need to be managed. For an e-krona to become established and be used, it is also important that it can normally be used on-line, like the payment services we are used to. Our tests have shown that e-kronor stored in the network can be used for payment services in the same way that we are used to today with our digital account credits.

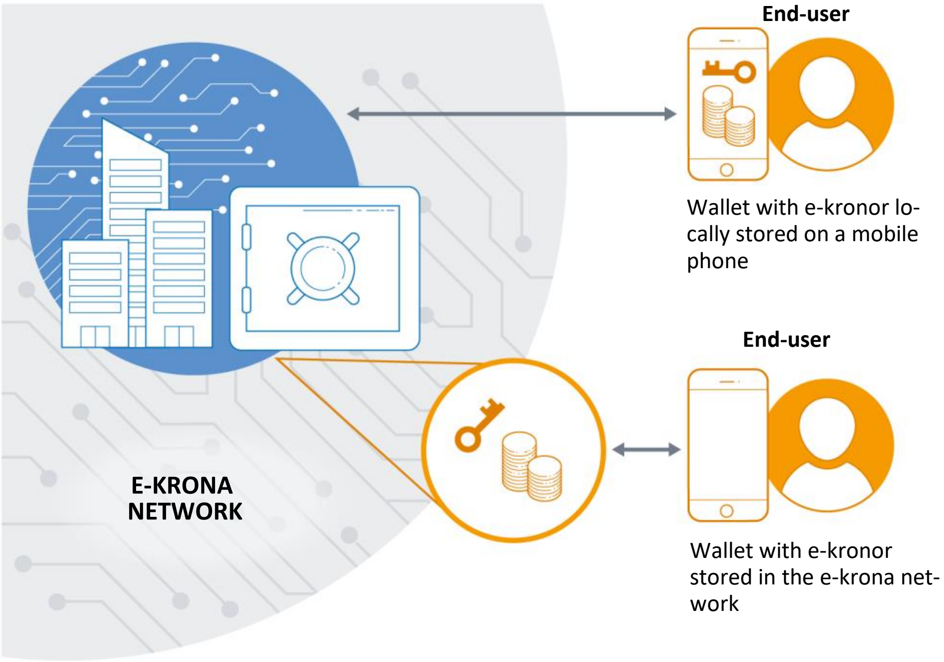
Different wallet models entail different opportunities

The report on the first phase of the e-krona pilot discussed the theoretical possibilities of a technical solution to store tokens and private keys in different ways. These so-called wallet models offer different possibilities and limitations in terms of payments. The wallet model where tokens and keys are stored on the network in the participant's node means that the same type of services can be offered as in today's banking system with digital account credit. When tokens with e-kronor and keys lie with the end-user participants, several payment instruments can be connected to the e-kronor. For example, you can connect one or more payment cards and a mobile app that are all linked to the same e-kronor. This would work in the same way as today, when we access our money via debit cards and apps. It is a possibility that has been tested during Phase 2. Because the e-kronor are in the network, a lost or broken payment instrument does not mean that the money is lost. The design creates an e-krona that is perceived to the end-user and has the same possible features as the digital account credits that we are familiar with today. Even though the underlying technology differs from traditional account-based solutions.

The wallet model with storage of tokens and keys in the payment instrument, in the pilot called *the local wallet*, is the more cash-like design, where the end-user holds both tokens with e-kronor and a key locally in the e-krona app. This type of wallet means that only the end-user has control over the e-kronor and the model also offers the ability to initiate payments off-line without access to the network.

Figure 4. Wallet models

The picture illustrates different designs of wallet models implemented during Phase 2. One model stores e-kronor and keys on-line in the network of the participant and the other stores them locally on the mobile phone.


End-user
Wallet with e-kronor locally stored on a mobile phone
End-user
Wallet with e-kronor stored in the e-krona network
E-KRONA NETWORK

Tested off-line functionality

The off-line functionality is intended to move tokens with e-kronor, keys to tokens, and the ability to validate transactions from the participant's node in the e-krona network to the end-user's mobile app. As described in greater detail in the report from Phase 1, the technology in the e-krona network is based on UTXO (*Unspent Transaction Output)*, where each transaction consists of one or more inserted tokens and results in a new token to the recipient (and possibly a token with change back to the payer).[10] By extracting the information and function that is performed in on-line

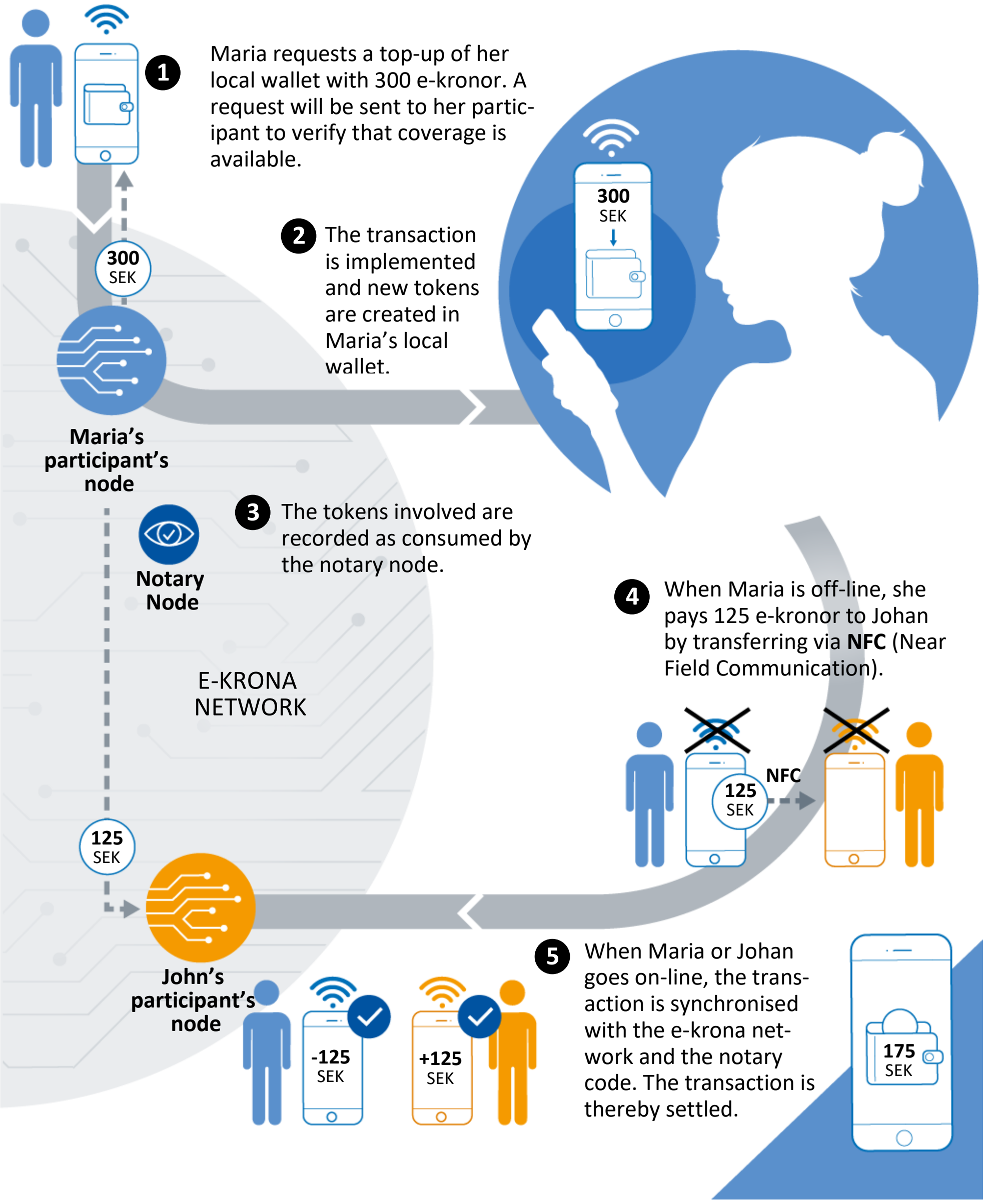
[10] In Corda, UTXO stands for *Unspent Transaction Output* which means that a token can be either consumed (spent) or not consumed (unspent). When a transaction is made, tokens that are not consumed are used as input tokens and thus become consumed. From the transaction, outgoing tokens are created that can be used in future transactions.

mode by the nodes in the network to the local mobile app, end-users' own mobile apps can create transactions with e-kronor using the locally-stored tokens and, for example, via NFC (Near Field Communication) transfer them to a payee. The payee's mobile app checks the authenticity of the e-kronor and that they originate from the Riksbank. The mobile app, as payer, needs to be able to create a transaction using the tokens inserted in accordance with the Corda's UTXO model, and as receiver needs to be able to validate the transaction chain that comes with a transaction.

The report from Phase 1 also explained the role of the notary node, to finally settle transactions in the e-krona network. The notary node checks that a token included in a transaction has not been used before, which would make it consumed. This function, which is intended to prevent double-spending, cannot be lifted to off-line. This means that transactions performed in off-line mode cannot be considered settled until the payer or payee goes on-line and synchronises the transaction with the network and the control of the notary node. Figure 5 shows an illustration of how e-kronor can be stored locally, used in off-line mode, and then synchronised on-line.

Figure 5. Transaction off-line

Illustration of how an off-line transaction works.



1
Maria requests a top-up of her local wallet with 300 e-kronor. A request will be sent to her participant to verify that coverage is available.
300 SEK
2
The transaction is implemented and new tokens are created in Maria's local wallet.
300 SEK
Maria's participant's node
3
The tokens involved are recorded as consumed by the notary node.
Notary Node
E-KRONA NETWORK
4
When Maria is off-line, she pays 125 e-kronor to Johan by transferring via **NFC** (Near Field Communication).
125 SEK
NFC
125 SEK
John's participant's node
-125 SEK
+125 SEK
5
When Maria or Johan goes on-line, the transaction is synchronised with the e-krona network and the notary code. The transaction is thereby settled.
175 SEK

Lessons and reflections on the opportunities and risks of the off-line functionality

The off-line testing has shown that it is technically possible to store the tokens and key locally in a mobile app and, using NFC, transfer e-kronor to a payee with updated balances for both. The transactions can then be synchronised with the network and settled when one party goes on-line again. It is also possible to handle multiple-step transactions off-line with multiple payer and payees in a flow of transactions. However, there are practical limitations as to how many consecutive off-line transactions can be handled by mobile phones, and there are also risks to consider, and the consequences and potential spread of these can be greater the more consecutive off-line transactions that are tolerated.

The transactions, as mentioned above, require synchronisation with the network and the notary node so that the tokens included in an off-line payment can be checked and thus the payment can be settled. If it is not possible to protect the data on the tokens stored locally on your mobile phone, there is a risk that an end-user might be able to access the information on your mobile and copy the tokens and use them multiple times in off-line mode. Such fraud is not easy to carry out and the risks can be minimised, but they cannot be completely ignored. However, even physical banknotes are not entirely risk-free because there is a risk of counterfeiting.

In the case of off-line payments, it is not possible to know with complete certainty whether a token with e-kronor has been tampered with or has been used previously, the so-called double-spending problem. This problem exists as long as you use unprotected hardware, which in this case a mobile phone is.[11] Another important insight is that a solution like the one tested in the e-krona pilot, whose security is based on the network detecting and stopping possible attempts at manipulation, is exposed to risks if transactions are allowed to occur outside the network's supervision, which is the actual definition of off-line transactions. Physical cash is not, of course, checked against any network when used in a transaction, but it is physically checked by the payee, which is not possible in the case of digital payments. Digital off-line payments need to be complemented by a regulatory framework that limits and manages risk. [12] Off-line transactions also make it possible, at least temporarily, to make transactions without transparency, which creates a risk of, for instance, money laundering and other criminal transactions. This is why an off-line function needs to be limited, given those risks in particular, even though the technology might allow more.

Examples of some issues associated with off-line activity and its risks:

- How much money should one be allowed to store off-line?
- What size transactions should be accepted?
- Should there be different rules for different e-krona users (e.g. consumers and merchants)?
- How many consecutive step-by-step off-line transactions can be allowed before an on-line synchronisation is needed?
- How long should a user be allowed to remain off-line?
- How should risks be shared when making off-line payments?

It would also be a technical challenge to apply the rules in a safe way, because any restrictions, like tokens, must be in the local mobile phone to work off-line. And then, like tokens, they need to be protected from manipulation.

[11] There is a lot of work on development of hardware that is designed to store data that needs to be very difficult to access and manipulate, so-called *tamper resistant devices*. For example, special cards, card readers, or safe areas on the mobile phone hardware. However, for off-line use to work on a mobile phone, an e-krona app must have access to the safe area of the hardware, which requires collaboration with the hardware manufacturer.

[12] There are currently examples of card issuers that allow their customers to make transactions off-line and where the associated risks of transactions are borne and handled by the card issuer.

As shown in the picture, the pilot implementation has been made so that the local wallet with the locally stored e-kronor is only intended for off-line transactions to other local wallets. However, there are no technical barriers to using a local wallet with locally-stored tokens even in on-line mode if desired. This is a conscious delimitation that we have made in the pilot and it is worth considering whether there can be a value in clearly separating money stored locally and available for off-line transactions, from those stored in the network.

One reason why this separation would be needed is that the locally-stored money will be lost if the owner loses his local wallet, or breaks it. As the wallet can be used for off-line transactions, it is by definition, for certain periods, without synchronisation with the network. If it is to be possible to get back locally-stored money when the payment instrument is lost or broken, there may be difficult situations where it is not possible to know with certainty how many e-kronor were in it during off-line mode. There are suggestions for solutions to minimise such problems, but they could be difficult to follow up in practice. A lost wallet with off-line functionality would therefore have to be regarded in the same way as lost cash. We see this as a problem that the existing technology has not been able to solve.

2.4 Integration with POS terminal

A fundamental objective of a possible e-krona is, of course, that it should be a functional and viable means of payment in daily commerce, like the current debit and credit cards and, in most cases, cash. A payment with the currently available central bank money, namely physical cash, requires only one payer and one payee for the payment to be initiated and settled. Today, however, the majority of payments in physical trade are made via point of sale (POS) terminals in accordance with the rules of the card networks and terminals. A digital payment with any kind of card involves a variety of commercial players (card networks, card issuers, terminal providers, etc.) all needed to make the payment possible. If the Riksbank is to establish an e-krona on a digital payment market in the retail trade, it will have to relate to the established commercial players and the existing rules and protocols.

An e-krona could have a very independent position, which would place higher demands on the Riksbank to design and manage specific e-krona equipment in the form of cards, terminals and regulations. With its own software, hardware and protocols, the e-krona could offer a completely independent payment solution, which would make the payment market more robust. The alternative would be to integrate it with the other players' hardware and standards. This would mean that the Riksbank would have less direct responsibility, but also become more dependent on commercial operators and their infrastructure, standards and business models.

There are currently standards for security and verification of chips in cards and software in payment terminals, where the most common, known as EMV, is used by the large card networks.[13] These terminals are often fully compatible with the cash and

[13] https://www.emvco.com/

accounting systems of retail stores and have high security should they be subject to attempts to manipulate hardware or software.

In Phase 2, the pilot has examined the various options available if the Riksbank wants to establish an e-krona on an existing POS market and has tested technical integration with a supplier whose POS terminals are on the Swedish payment market. The aim was to technically test how an e-krona in a separate network could be used on terminals that are currently available and that process payments on the large card networks with their protocols.

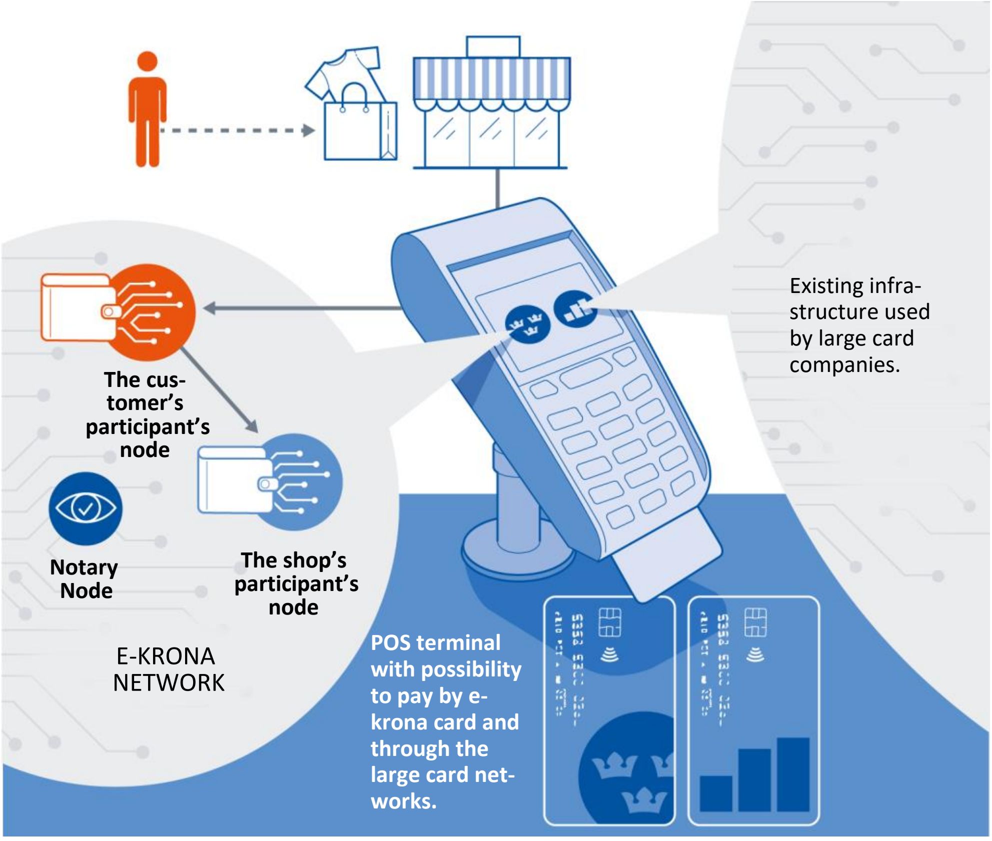
Tested POS integration

During Phase 2, a POS integration was tested, whereby special software for the e-krona was installed in the terminal so it could support e-krona payments in the e-krona network. These payments are processed separately from the traditional card payments that can be made in the same terminal. The Riksbank is then responsible on its own for the software, the certification of the terminal suppliers and the security solution for the terminals. The structure requires the Riksbank to reach out to the terminal suppliers, sign contracts with them and certify them. In addition, the Riksbank must be responsible for developing and managing the software and security solution necessary for the use of the e-krona in the terminals.

When the e-krona is integrated into a terminal, suppliers may have different rules and principles for communicating out of the terminal. The terminal we have tested allows communication directly from the terminal to the e-krona system. Other suppliers may have completely different rules on communication via their hardware, which may make the e-krona dependent on these actors' IT infrastructure.

Figure 6. Payment in POS terminal

Illustration of how e-krona specific software has been implemented in a POS terminal that enables payments with e-krona and other card networks in the same terminal. The end-user initiates purchases with e-krona against the store's terminal, which communicates directly with the e-krona network. The payment is made through the nodes of their participants in the network.


Existing infra-structure used by large card companies.
The customer's participant's node
Notary Node
The shop's participant's node
E-KRONA NETWORK
POS terminal with possibility to pay by e-krona card and through the large card net-works.

Lessons and reflections from the POS activity

If an e-krona were to be launched, it would mean that the Riksbank would issue a payment fund in a payment market where there are existing actors and established standards for how payments are made and how their security is guaranteed. This is a clear difference from today's cash which can be used more independently. For e-krona payments to be accepted in commerce, it is a great advantage if they can be integrated as smoothly and cheaply as possible for the retail trade. Adapting the e-krona to the standards already used by the major networks on the card market could facilitate its establishment and reduce the Riksbank's work on setting up its own software, regulations, procedures and administration. On the other hand, it is no small task to fully integrate an e-krona into these card networks, and a parallel solution might also have its advantages, as it can make the payment market more robust. Swish is an example of an independent payment solution that is increasingly becoming established as a payment instrument in the retail trade and is not covered by the regulatory framework for the card networks. The POS activity in Phase 2 was conceptually similar, but as solely technical activity without an established regulatory framework.

The testing in the e-krona pilot has shown that it is possible to integrate the e-krona network by implementing e-krona specific software and flows on an established terminal that also handles the large card networks, which means that a merchant with the terminal can receive payments with e-kronor and payments via the large card networks on the same terminal.

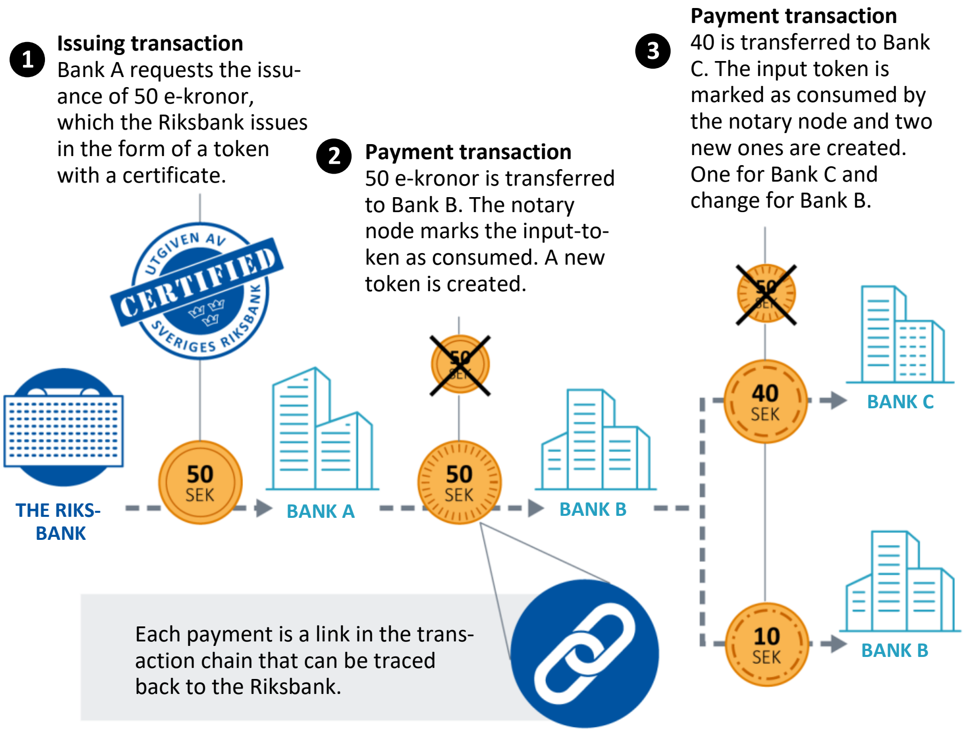
The idea of what can function as a payment terminal is also changing at the moment, where developments are moving toward the possibility of using ordinary mobile phones as safe terminals. This can create increased opportunities and flexibility for how payments in the e-krona network can be integrated into the retail trade. By avoiding the card networks' standards, some complex issues are avoided and more freedom is given, which has been demonstrated by Swish, for example. If one looks to the rest of the world, one can also see that the major initiatives in the payment market, both within CBDC and other initiatives, are focusing on mobile payments. Regardless of which payment instruments could be used for an e-krona, regulatory frameworks and collaboration with retail trade operators are required to establish the e-krona as a means of payment. For the forthcoming work on the e-krona, it will be important to continue investigating potential collaboration models with market participants and also working on making the e-krona flexible to follow developments in the payment market.

2.5 Performance tests

One of the most important requirements for a potential e-krona is that it can be used for digital transactions in real time. In the e-krona pilot, the e-krona and its network are based on a technology that has not yet been used in production for the purposes, transaction amounts and patterns that an e-krona would entail. An important focus area during Phase 2 was to continue testing performance and to examine specific characteristics of the solution that could have an impact on its ability to perform real-time transactions. The e-krona in the technical solution we are testing is designed as a so-called token, which represents a certain value in e-kronor issued by the Riksbank. Each transaction with e-kronor consists of one or more tokens (input) with e-kronor from the payer that result in an output token to the payee with a possible output token with change given back to the payer. The tokens used as input in a transaction are marked as consumed and the e-kronor are passed on to the payee in the form of a new output token that can be traced back to the input tokens where the e-kronor were previously held. In this way, each transaction creates a link to transaction chains within the e-krona network with traceability to the Riksbank as the issuer that guarantees the authenticity of the e-krona. This is done by the network participants and is not visible in any way by end-users, who are unaware of how many tokens their e-kronor total consists of and the transaction chains of these tokens.

Figure 7. Transaction chain

The figure provides a simplified illustration of how transaction chains are created in the technical solution, where each token has traceability to the Riksbank as issuer of the e-krona.



1 **Issuing transaction** Bank A requests the issuance of 50 e-kronor, which the Riksbank issues in the form of a token with a certificate.

2 **Payment transaction** 50 e-kronor is transferred to Bank B. The notary node marks the input-token as consumed. A new token is created.

3 **Payment transaction** 40 is transferred to Bank C. The input token is marked as consumed by the notary node and two new ones are created. One for Bank C and change for Bank B.

Each payment is a link in the transaction chain that can be traced back to the Riksbank.

Note. The individual tokens in the figure have different patterns to illustrate how they are unique and their traceability in a historical transaction chain

The participants in the network check that the e-kronor are genuine and can be traced to the Riksbank and the notary node checks that a token has not been used before. The fact that the e-krona in this solution is designed as uniquely identifiable tokens that can all be traced to the Riksbank means that it is in some ways similar to physical cash. One such similarity is that only the Riksbank can create the e-kronor and thus they become easy to distinguish from other digital money. However, the associated transaction chains mean that the transactions are more complex than in more proven account systems. This can reduce the solution's ability to achieve the same performance as traditional solutions.

To give a simple example: A transaction of SEK 100 in the tested solution can consist of a token with a very short historical transaction chain, which means a small amount of information to validate and verify. But it can also consist of a variety of different tokens with different lengths of historical transaction chains, which means a greater amount of information to validate and verify. Traditional account-based systems that are not based on uniquely identifiable money do not have the same kind of information in a balance, and thus do not have as much variation in the amount of information that accompanies a transaction.

During Phase 1, a first performance evaluation was carried out, which tested whether it was possible to carry out, during a period of 10 minutes, on average 100 mixed transactions per second, with 100,000 users. This proved possible, but then the transactions were simple and lacked a larger amount of tokens with complex chains of transactions. During Phase 2, more advanced and challenging tests have therefore been carried out. They have been designed to be a little more “messy” and realistic in the composition of tokens, for example, which can affect performance. The overall goal has been to investigate whether the solution could handle transaction volumes equivalent to those of Swish and the larger card networks at peak times and be able to keep the average time for a transaction around one second. The tests have been conducted in a limited test environment, limited to the e-krona nodes without links to the payment instruments of the end-users and the alias service.

The purpose of the tests was to examine which characteristics of the technical solution and which scenarios could cause problems in the case of instant transactions. The performance tests investigated the following:

- What amount of transactions per second can the simplest scenario complete? The simple scenario means that the transactions consist of a few tokens without long transaction chains.
- How does the length of the transaction chain affect the speed of a transaction?
- What effect does the number of tokens have on the network and on the transaction speed (the question is most likely to be relevant for larger deposits/exchanges)?
- How do different types of transaction (issuance by the Riksbank, withdrawals and deposits from customers, transactions within the network and redemption at the Riksbank) affect the network's ability to deliver instant transactions?

Lessons and reflections from the performance work

The tests show that in the simplest scenarios, the implemented solution in the delimited test environment can deliver transactions per second well in line with the peak load of Swish and the card network. However, these scenarios are not likely in a system that has been running for some time. The system will then consist of many tokens divided into small and large values and associated chains of transactions, which means more information to validate in the transactions. As the tests become more complex, for example in terms of the length of the transaction chains and the number of tokens in the transactions, it becomes more difficult to achieve a certain performance. It is above all when the chains become very long and in test cases when the amount of tokens increases significantly, that there are problems with performance. This applies both to transactions within the system and when e-kronor are to be redeemed at the Riksbank again. When a wallet contains many tokens, it also takes longer to choose which tokens to include in a transaction. In addition, it was noted that it takes a long time to add up a balance to be displayed in the app, for example, when a wallet has thousands of individual tokens. [14]

For an average individual with an e-krona wallet, the probability is low that the wallet would contain as many tokens as in these examples.[15] However, for a business operator who should be able to receive e-kronor payments in daily commerce, the amount of tokens will soon grow large. These challenges also show the fundamental difference between the tested token solution, built on a UTXO model, and a traditional account model. In that type of account model, slightly simplified, it is only the balance that is listed and a data record for a transaction that is added, while the token model has to verify, save, update and track a varying amount of data objects.

Designing tests with more realistic scenarios is difficult, not least because it is still unclear exactly how an e-krona would be designed and what role it would play in the Swedish payment market. The biggest performance challenges arise when the payment chains create a fragmentation of tokens that increase the amount of tokens in the network and the payments. The exact nature of this fragmentation is difficult to know in advance. The purpose of the performance tests was to understand the situations in which the solution with tokens and transaction chains can cause performance problems. The tests have given us a good idea of this and during the course of our work we have also discussed from a theoretical perspective how such problems could be avoided.

The proposed solutions are to design a more intelligent management of the wallets and their tokens. For a retail trader who has received a lot of payments with tokens, a regular merger of these into a larger token or regular deposits could prevent performance problems. For a participant who often receives requests for withdrawal of e-kronor from end-users, it may be more optimal to have a greater variety of tokens with different amounts of e-kronor. Automatic redemption and exchange of older tokens with long transaction chains also reduces the amount of information to be managed in transactions, which could benefit performance. The proposed measures would need to be further investigated to ensure that they do not affect users' ability to use their e-kronor. Further investigation would also be needed to understand the other consequences of the measures for the technical solution and the conceptual model.

One important thing to remember is that an e-krona solution like the one in the pilot consists of several different components, all of which affect the performance of the solution. During Phase 2, much of the work to improve performance was devoted to optimising the e-krona engine and managing databases. Performance work is also a continuous process that all possible technical solutions would have to work with to ensure scalability in the system as the volume of transactions increases. It is also worth emphasising that work in the pilot Phase 2 has been built on version 4 of Corda

[14] The version of the Corda platform on which the e-krona pilot is built also has a firm limit, which means that a transaction may consist of at most 10,000 tokens.

[15] During the performance work, large-scale simulations have also been carried out to investigate how tokens and associated transaction chains could develop at users of the system.

and that the platform is constantly being improved, not least in terms of performance and scalability.[16] For the pilot, the work has been rewarding and helped us identify the potential challenges that solutions of this kind can have. Some lessons are likely to be more specific to this particular solution and its implementation. Other lessons are more general and can be used in the further work of comparing different potential solutions.

3 Legal work Phase 2

The legal analysis was based on the technical solution in the e-krona pilot and the legal analysis carried out in Phase 1. The analysis in the project shows that the data accompanying the transaction chain is likely to be considered as data that is subject to financial confidentiality and personal data that is subject to data protection regulations. Furthermore, in Phase 2, we have continued the analysis of which type of asset the e-krona can be regarded as, reaching the conclusion that it could be seen as an electronic form of cash, and thus a new alternative and complement to the physical form of cash that exists today – banknotes and coins.

3.1 The e-krona, financial confidentiality and personal data protection

The type of DLT/block chain technology used in the e-krona pilot's technical solution is to verify that tokens are genuine through the transaction history that accompanies it to the recipient's payment service provider. This means that more information is shared between the participants in the system than in traditional payment systems. During Phase 1, the project noted that there was a need to investigate how this sharing of information relates to financial confidentiality (used hereinafter as a concept for both banking secrecy and confidentiality under the Payment Services Act) and to data protection for personal data.

It is the participants in the e-krona network who are obliged to observe financial confidentiality. This means that participants are not allowed to disclose customer information to unauthorised persons. As far as data protection regulations are concerned, it is a question of whether the processing in the network meets the requirements of the legislation. The rules concern, among other things, the purpose of the data processing and various rights for end-users, such as the right to have data erased.

[16] Corda 5, which is about to be launched, will include improvements in performance and scalability.

It is unclear how the existing law on financial confidentiality and data protection for personal data relates to DLT/block chain technology. This is an area in which it is reasonable to interpret the legislation with caution, given the rights and interests that these rules are intended to protect. The analysis in the project shows that the data accompanying the transaction chain is likely to be considered as data that is subject to financial confidentiality and personal data that is subject to data protection regulations.

As the technical solution tested in the pilot is designed now, one cannot rule out the possibility that data in the network is processed in a way that is not compliant with the legislation on financial secrecy and data protection. Legal amendments and/or information security measures may therefore be required, if the solution tested is to comply with relevant legislation. Consultation with both the Swedish and the European Data Protection Authorities may be necessary to clarify how a solution based on DLT/block chain technology relates to data protection regulations.

3.2 E-krona - an electronic form of cash

During Phase 1, we compared the e-krona as a means of payment with the means of payment we have now. Because of the way the e-krona was designed in the pilot, we considered in the legal analysis that the e-krona showed the most legal similarities to cash. During Phase 2, the legal analysis of the solution has been deepened and a proposal for the formulation of legal principles for the e-krona has been drafted, see Appendix.

A fundamental question has then been to analyse what legal status physical cash has today and what this could entail for the e-krona in the pilot solution. The project has carried out this further analysis with the help of a legal expert in payments. The conclusion of this analysis is that physical cash has historically been a debt instrument, and that the holder has been entitled to a certain amount of metal in exchange for the value represented by the cash. However, physical cash can no longer be considered to represent a claim in the legal sense, but is instead a means of payment with an independent value (*sui generis*), which represents economic power/purchasing power. This is shown by the fact that physical cash is not interest bearing and cannot be subject to statutory limitation provisions. Nor is there any longer a direct requirement that the holder of a banknote or coin can impose on the Riksbank, for example, the issue of a special metal. It is instead a relationship that can be said to be based on confidence in the state as guarantor of the value of the cash.

Like physical cash, the e-krona in the pilot's solution represents economic power/purchasing power. According to the analysis, it may be regarded as an electronic form of cash, which is seen as a new alternative and complement to the physical form of cash available today – banknotes and coins. In the pilot's solution, it is intended that the e-krona should be protected in the event of a participant's bankruptcy, since it belongs to the end-user. Participants ensure that end-users can complete transactions in e-kronor and exchange e-kronor for other types of money. However, the e-krona should not be included in the participant's assets once the end-user has paid for it. If the pilot's solution were to become a reality, this means that new legislation would need to be put in place to ensure that the e-krona is given the protection and legal status described here.

Having possession of physical cash entails certain legal consequences. When it comes to the e-krona as electronic cash, the holding could instead be linked to the registration in the electronic wallet. The wallet is the instrument where the e-kronor are stored, a kind of information account (this may also be relevant for other payment instruments). This means, for instance, that it does not have any direct legal significance where the keys to the electronic wallet are located, which was something we considered during Phase 1. The choice of technology thus would not directly affect the legal design, which would instead be technology neutral.

Since the e-krona in the pilot solution could be considered to belong to the same asset class as cash, it follows that the rules relating to claims are not applicable. This means that the e-krona cannot, in that case, be interest bearing or the object of statutory limitation provisions in accordance with the legislation applicable to debt instruments.

If there is reason to limit the size of the holdings of the e-krona, or to provide incentives to hold e-kronor, such instruments could be introduced in the form of either limits on amounts or fees/compensation linked to the electronic wallet.

4 The continued work on the e-krona

The project is now entering Phase 3. The work has provided the Riksbank with valuable information on the opportunities and challenges of the solution tested. It has also been a good basis for investigating general technological and policy-oriented questions, and also the legal framework for an e-krona. Phase 3 will continue to test specific parts of the technical solution, but also focus on preparing the vision and requirements for an issuable e-krona.

4.1 The ability of the technical solution to offer programmable money and payments

DLT- and token-based solutions are often said to have an advantage over more traditional solutions if you want to foster innovation in payments. Concepts such as *programmable money, smart money* and *smart payments* are often said to be the future of payments, and this is used as an argument in favour of the new technology. The meaning of these concepts may vary, but they aim to create new, efficient ways of making payments and money for special purposes through programming. The e-krona pilot has not yet looked specifically at whether, and if so, why exactly DLT- and token-based solutions would benefit innovations in payments. However, the technical work in Phase 3 will focus on this particular area. We want to test and explore how such solutions can be used to create new payment services, and why they would be more effective than more traditional technologies. We also want to examine whether it would be possible for market participants to create innovations without risking the fundamental characteristics of the e-krona, and without the Riksbank as the issuer of the e-krona having to be directly involved. We want to gain a deeper understanding of how much substance there is in the frequent arguments in favour of the new technology, and whether they are relevant to a potential e-krona.

4.2 Collaboration model for an e-krona

As we have already mentioned, an e-krona as in the tested model would require collaboration between the Riksbank and market participants. The distribution model with the participants and the POS activity are two areas that have been technically tested during Phase 2. This type of collaboration with several different types of actors also requires some form of collaboration model that defines the roles and responsibilities of the different parties. If the e-krona is to be dependent on private actors, it needs to have a place in their operations and business models. The topic also covers issues regarding the Riksbank's organisation for the operation and management of an infrastructure in which the Riksbank interacts with market participants. During Phase 3, the questions surrounding the cooperation model will be investigated in more detail.

4.3 Legal questions

There are several questions to be investigated further in the legal work. One important question is to consider whether the e-krona system should be regarded as a settlement system, another is to determine when a payment is settled. This must be clarified to avoid systemic risks arising. In the pilot, the starting point is that the settlement of the payment should take place instantly and that the e-kronor should not be included in the bankruptcy of the participant/intermediary; the question is therefore what systemic risks can actually arise in the system. If it is to be regarded as a settlement system, it has an impact on who can participate in the e-krona network.

One question that was identified and analysed as early as in Phase 1, and which there is reason to further analyse, is how to handle operational risks and a potential default of a participant. In this context, it will be interesting to discuss who owns the information in the system, and on which cooperation model a solution can be based.

Within the framework of the legal work, the project will also continue to investigate and analyse the legal design of an e-krona.

4.4 Design and requirements of an issuable e-krona

During the year, the Riksbank will also focus more on how a possible e-krona would look and function. We will therefore devote a great deal of time and resources to producing such proposals. All of the tests, analyses and investigations carried out so far will form a base for this work. Part of the work will involve comparing the technical solution that has been tested with other possible solutions for a launched e-krona. In the spring, therefore, a *Request For Information (RFI)* will be sent out, where market participants will be able to describe how their proposed solution could work for an e-krona. In addition, the project will gather views from various actors in the payment market and from the general public.

APPENDIX – Proposal for the legal design of the e-krona

The e-krona– a dematerialisation of physical cash

Below is a proposal for a legal design of the e-krona based on a dematerialisation of physical cash:

A means of payment issued by the Riksbank

- Physical cash and digital cash – "e-kronor" – shall co-exist and complement each other.
- The e-krona shall constitute legal tender and be an official representation of the Swedish currency (krona) in the same way as physical cash.
- The Riksbank shall have the right to issue cash as a means of payment in physical and digital form. The e-krona entails a dematerialisation of physical cash.
- Only the Riksbank shall be able to issue and redeem e-kronor. It is important that the central bank (the state) is the sole principal and that the e-krona is not commingled with private alternatives.
- The Riksbank's task is to safeguard the functionality and value of e-kronor.
- The amount of e-kronor issued shall be booked as a liability item in the Riksbank's balance sheet in the same way as physical cash. E-kronor shall have the same value and legal status as physical cash, i.e. be the digital version/representation of the currency (krona).

Functionality for the e-krona

- The Riksbank shall provide the payment system that will enable transactions in e-kronor. E-kronor can be used by the public, companies (financial and non-financial) and authorities as end users of the means of payment.
- E-kronor shall be subject to requisite money-laundering controls.
- Riksbank shall have the exclusive right to issue e-kronor.
- It is mainly intermediaries that will connect end users, distribute e-kronor to end users and enable transactions between end users.
- When the end user has paid for e-kronor, they are stored in an electronic wallet (a digital storage area) or other designated payment instrument such as a debit card.
- The electronic wallet and other designated payment instruments are mainly provided to the end-users by intermediaries. E-kronor shall be the property of the end-user after they have been placed in the end-user's electronic wallet.

- E-kronor may not be included in the asset base of the intermediary after they have been placed in the end user’s electronic wallet (or any other designated payment instrument) and shall be protected in the event of the intermediary's bankruptcy.
- E-kronor shall be able to be used by the end user for payment and other transfers. Payments shall be able to be made instantly.
- An end-user shall be able to purchase and redeem e-kronor for other types of means of payment from the intermediary.

Robust and available in both normal and peacetime crisis situations and during a heightened state of alert

- In order for the e-krona to be robust and efficient, in both normal and peacetime crisis situations and during a heightened state of alert, the Riksbank shall be given the legal right to govern and control the distribution, availability and functionality of e-kronor. This should be done through the Riksbank being authorised to own infrastructure, to impose requirements on intermediaries, end users and other agents, and to decide what functions an electronic wallet shall have. In order to achieve this, the Riksbank should be given the right to make decisions, issue regulations and conclude agreements on matters relating to the e-krona. The Riksbank has similar powers with respect to physical cash today.

Regulation

- The e-krona can probably be regulated without amending the constitution, but it may be appropriate to make the constitution technologically neutral (today the issuing monopoly is linked to banknotes and coins) and to clarify that it is only the Riksbank that is allowed to issue an e-krona. In addition, certain amendments are required to Chapter 4 of the new Sveriges Riksbank Act (Bill 2021/22:41) which regulates the Riksbank's mandate with regard to cash and other means of payment and the position of cash as legal tender. Then there would be a need for a concise law addressing the civil law conditions for and effects of allocations of e-kronor (compare in particular Chapter 6 of the Act on Central Securities Depositories and Registration of Financial Instruments) (1998:1479). This act may either be independent or may be inserted as a separate chapter in the new Sveriges Riksbank Act.

- The Riksbank shall be able to issue rules and regulations for technical or monetary restrictions on the electronic wallets and/or charge fees or provide compensation for them if the Riksbank considers this to be appropriate.

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

PRODUCTION SVERIGES RIKSBANK
ISSN ISSN. (on-line)