SUMMARY

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

REF: 2022-00632

DIALOGUE FORUM E-KRONA

DATE: 07 December 2022

DOCUMENT RB PUBLIC

CLASSIFICATION:

PRESENT: Mithra Sundberg, Riksbank, Chair
Gabriela Guibourg, Riksbank
Anders Mölgaard Pedersen, Riksbank
Lars Andersson, Riksbank
Carl-Andreas Claussen, Riksbank
Fredrik Rydbeck, Riksbank
Elisabeth Nilsson, Riksbank
Birgitta Söderlund Rietz, H & M
Harry Rymert, SEB
Jenny Winther, Handelsbanken
Johan Hörmark, SEB
Johan Weijne, Bankgirot
Oscar Berglund, Trustly
Robin Teigland, Chalmers University of Technology
Susanna Laurin, Funka

Meeting 5. Contingency and offline payments

Introduction

The fifth meeting of the e-krona dialogue forum was about contingency and offline payments. The Riksbank's working hypothesis is that an e-krona should strengthen the resilience of the payment market, especially during a societal emergency (crisis during peacetime) or during a heightened state of alert. The e-krona needs to function independently of central systems in the event of longer disruptions to the power supply and data communications in order to function in these situations. Such an offline feature may also be beneficial even in the event of minor disruptions under normal conditions.

Prior to the meeting, some of the participants had been asked to make a presentation based on the perspective they represent. The discussions were divided between banks/payment service providers and retailers.

Banks/payment service providers

What are possible lessons learned from banks and other payment service providers work to secure payments?

The work and possibilities to secure payments depend on where in the transaction chain disruptions occur and their duration. If outside of PSPs' scope, this is regulated in SLAs and customer agreements; if within PSPs´scope, contingency plans, etc. exist. The participants considered that short-term disruptions usually do not pose any major problems, but that a long-term interruption would create major problems for the whole of society and it is difficult to develop digital systems capable of handling this. It was noted that the offline concept may relate to different types of situations in different parts of the transaction chain. For example, it could be that all telecommunications are inoperative or that there are disturbances along the way, e.g. in clearing systems, disturbances in a client's internal systems, or in the bank's own system.

The Riksbank could draw inspiration from the card systems' arrangements for offline payments, clarifying liability rules and responsibilities. Participants suggested that much can be addressed through proper design and clear regulations for offline payments. For offline card payments (as for an e-krona), important parameters that involve trade-offs are amount limits and frequency of reconciliation.

A core element of the scheme rules for offline card payments are flexibility for retailers – but this involves trade-offs as well. It was mentioned that an e-krona system could be designed so that the recipient of an offline transaction can choose whether to accept the transaction or not, thus addressing the uncertainty of offline transactions. The situation was compared to purchases at card terminals that are offline (for example, when making a card payment on an airplane). It is then up to the recipient to decide how much risk they are willing to take. Participants argued that a sender of an offline payment probably does not need to limit the amount or the occasions to send offline payments, but the recipient will always prefer payments to be made online.

How can an e-krona complement PSP:s contingency arrangements – and vice versa?

Participants argued that a large degree of system and payment solution redundancy already exists, both within and outside PSP:s, e.g. in the connection to SWIFT, to the network, to clearing and settlement systems, and to banks' internal systems. There are already services that overlap - for instance parallel data centres, consumer applications that can support the user experience, and Swish that separates clearing and settlement infrastructure. A parallel end-to-end solution will of course add redundancy, but will come with a cost and require activation criteria. It will be necessary to define to what extent and in which scenarios an e-krona would work as a backup solution.

Participants discussed that a PSP's involvement in an e-krona as a backup payment solution should be incentive-based. All parties involved in the transaction chain need to see the benefits of integrating the e-krona system into the current system. Consumers need to see clear benefits, for example in terms of convenience, speed or cost saving. PSP:s need to see benefits such as lower costs, accessibility, kick-backs or high demand for e-krona. In addition, there need to be a high level of availability and interest for retailers to accept this type of payment.

Participants argued that even if payment services are parallel, the infrastructure needs to be parallel to achieve a true backup solution, but that this is probably not cost effective.

Participants also discussed in general terms how a parallel infrastructure could work. For example, there could be an infrastructure that is only activated when needed. This could be in the event of longer disruptions of existing infrastructure and/or when the government decides on a specific level of alert. However, it will be difficult to know that the system will actually work in an emergency. One idea would be to regulate how often the system would go online even in normal times. It might not necessarily need to be online all the time, or have some sort of levels when payments should be made online/offline. This could make the system faster and ensure that the system will always work, even offline, because it happens regularly regardless.

Participants mentioned that a flat hierarchy should be built, allowing for many different channels of reconciliation with the central register.

Another point mentioned was that from a risk perspective it is important that traceability is also available offline. One can also imagine some advantages of a certain slowness in the system when it comes to crime prevention.

Retailers

The discussions from the retailer perspective were based on different scenarios. They envisioned what would happen in a physical store and on a website via e-commerce in cases where the retailer lacks electricity or data connectivity.

In a physical store

In case of a power outage, many retailers will have to close very soon (e.g. within an hour) for various reasons, and an e-krona as a possible backup solution would not be relevant. Participants told us that they have the capacity to keep the store open for about an hour. After that, the battery life of the backup systems would run out and the store would have to be closed for security reasons. For example, it would not be possible to remove security tags, handle large amounts of cash, neither handle receipts nor refunds.

In case of loss of data connection (for example, in the event of a cyber-attack), but where there would still be access to power, certain payment solutions could still work, and an e-krona could be a further backup solution if available offline. The store can still accept cash, some card payments and 'buy now pay later' options (such as Klarna in-store). However, it would not be possible to carry out certain services or sell online tickets. Here, participants see a potential role for the e-krona if it can be used for offline payments. In this case, the credit risk would have to be managed in some way and possible limits would have to be considered. The e-krona also needs to be easy to use and readily available when needed.

E-commerce

In the event of a power outage, other servers may take over and there would be "no issue" and therefore no relevance in discussing a backup payment solution. There are back-up servers and it was deemed unlikely that both would suffer power outages at the same time. The website would not work at all and an e-krona would not help in such an event.

In case the internet page is down, customers are referred to physical stores. Again there is no relevance in discussing a backup payment solution. This scenario would also be unlikely but could happen, for example, in the event of a cyber-attack. Participants imagine that in this case they would try to refer the customer to the physical shop instead. It could also be that the connection to the payment service providers or the card acquirers does not work. The e-trader's website would still work, but the payment would not be completed once the customer reaches the checkout. Either the payment service would not work or the card payment would not go through.

Other issues discussed from the retailers' perspective were that they do not have the same requirements as, for example, banks when it comes to redundancy. The consequence is that back-up solutions is not something retailers have had to put much emphasis on. The problems and solutions probably differ between stores. In a grocery store, problems arise when item systems fail, but in retail stores there are price tags on each item so the correct price can be read at the checkout. The ordering system can then run afterwards. The reserve time of one hour of battery life can certainly also differ between stores. Participants suggested that higher standards could be set for the battery life of card terminals and that it would be useful to create e-krona terminals that can last longer without power.

Planning ahead

Three meetings are scheduled during spring 2023. The next meeting will be held on 23 February. Topics that will be discussed at future meetings are anonymity and integrity, cross-border payments, communication strategy, and work on the Riksbank's user survey, etc. It is likely that there will also be reason to discuss business models further, as well as discussing the results of the ongoing parliamentary payment inquiry report.