G+D
Currency Technology

Giesecke+Devrient's (G+D) value proposition to the Riksbank's e-krona project

www.gi-de.com

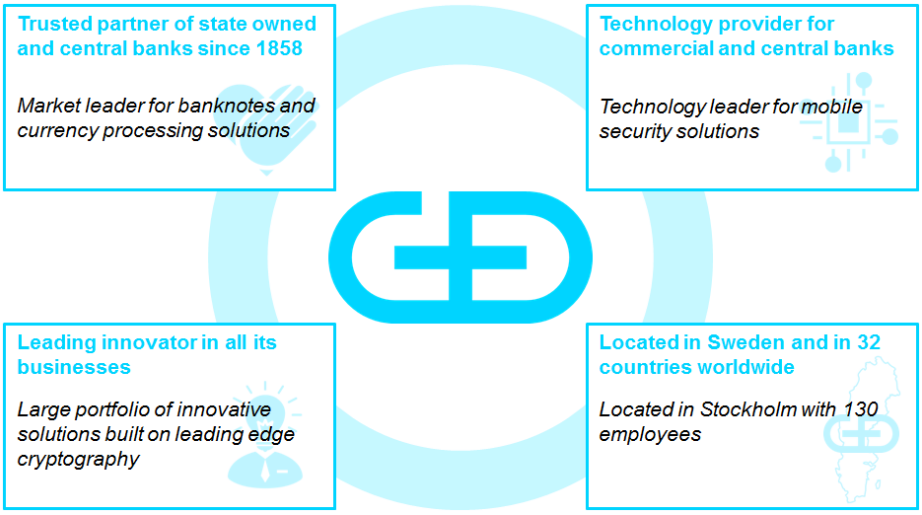
Introduction

We understand that Sweden may become the first country in the world where cash is no longer used. This obviously presents a certain number of challenges. Given that cash is currently the only means of payment that Riksbank offers the general public, questions around Riksbank's role in a society that is going digital obviously arise. For instance, should Riksbank leave the payment system in the hands of commercial banks and focus on regulation or should it play an active role in supporting the population on their digital journey?

Commercial banks are governed by commercial interests. It is unlikely that they feel a strong sense of responsibility for guaranteeing stability of the payment system as such or for including everyone in it.

A digital version of the krona, an e-krona, could be Riksbank's contribution to a future, completely digitalised payment system. This would increase competition and ultimately stability, especially in times of financial unease. But a digital currency such as e-krona also entails risks that are not yet fully understood. And the extent to which these risks may materialise of course also depends on the technical solution chosen to support and deliver this digital currency.

G+D is a long trusted partner of central banks and technology leader for electronic payment solutions

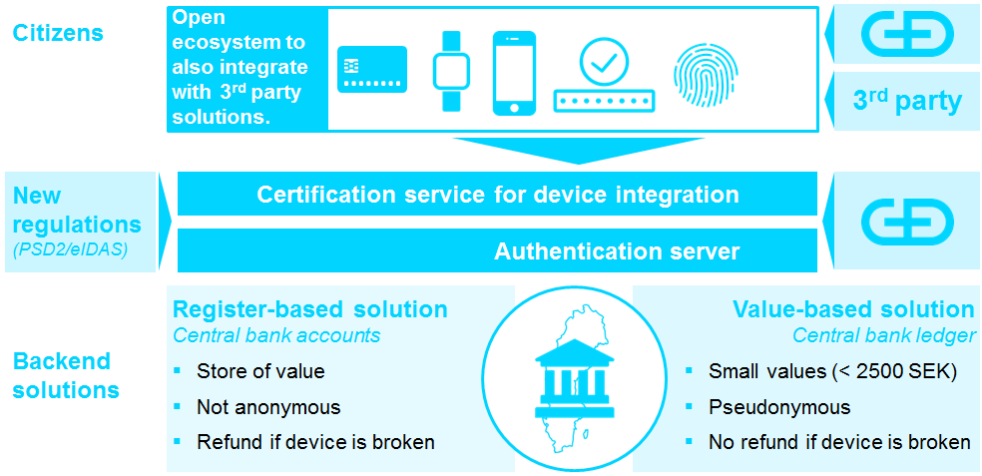


We are a trusted partner to state-owned and central banks since 1858 with long-term business relationships built on banknotes, security features and banknote processing systems.

We have a decade-long business in highly secure transaction and authentication methods including smart cards, secure wearables, secure app technology, cyber security solutions, data analytics and many more.

We are a global company with an important subsidiary in Stockholm employing approximately 130 people. This strong Swedish footprint, backed by a global technology network, means that we are able to integrate the latest leading-edge solutions from global markets while addressing the special needs of Swedish society.

Our proposed solution – Register- and possible value-based solution



Foundation for a register-based e-krona solution

A register-based e-krona solution would be built on a backend system similar to a conventional banking system. A middle tier authentication layer would sit on top of this, handling connectivity with the consumers' access devices – including smart phones, wearables and cards. As payments would be irrevocably settled within seconds with this register-based concept, a crucial infrastructure building block would be a highly secure frontend supporting strong but nonetheless convenient authentication processes. This calls for a **user-friendly, ultra-convenient mobile payment experience enabled by the latest authentication and app security technologies.**

G+D's mobile authentication solution is an open platform based on the FIDO (Fast Identity Online) industry standard. Highlights include:

- Leading-edge authentication methods: silent authentication from registered devices, cards, wearables, passwords/PINs and/or biometrics (fingerprint, face, voice)
- Authentication policies that can be customised either on demand by the consumer or centrally based on specified conditions (such as amount, time and location); policies could specify for instance card and phone for payments above a certain value or at night.

In addition, G+D's Trusted Application Kit (TAK) hardens payment apps against attacks. In general, secure elements and trusted execution environments are used to protect credentials when consumers authorise payments. However, hardware-based security is not present or accessible on many phones. To overcome this challenge, G+D has developed a pure software solution, the TAK. This kit protects smartphone applications against tampering by users or malicious applications. TAK uses whitebox cryptography, device fingerprinting, obfuscation and anti-tampering mechanisms to protect cryptographic keys and algorithms using these keys along with critical application code.

These authentication and security solutions from G+D would give consumers the flexibility to customise their authentication policy. So, for instance, consumers could specify that they authenticate payments by tapping a card against their smartphone (connection via NFC). They could also use a wearable such as a wristband instead of a card for this purpose. So all users would need to do is tap their phone against the wristband to authenticate a payment, enabling a very convenient and secure experience. For lower-value payments during the day, consumers might set their authentication policy to smartphone without the card. Or they may decide to pay for their morning coffee with just the wristband and no PIN by setting the policy to wristband-only on weekdays between 7am and 8am for amounts below 50 SEK.

Value-based e-krona solution synergising the register-based approach

A value-based solution would have the advantage of eliminating the need for users to register. They can simply download a wallet app or obtain a card or wearable with the wallet app software pre-installed. Then they charge e-kronas for immediate usage including offline payments. There are a lot of similarities between a value-based scheme and cash.

In order to leverage synergies across both schemes, the value-based e-krona should – at least on the consumer's end – be combined with the register-based solution to the maximum extent possible. To achieve this, we propose a "value-based solution with shadow accounts".

- A central database or blockchain manages the balances of e-krona wallets. In other words, each wallet has an entry in the database that identifies the wallet and stores the amount (shadow account). The wallets themselves are stored locally on devices with a pseudonymous identifier to access the backend system, e.g. the public key of a private/public key pair.
- An offline payment is realised by transferring a "signed IOU" from the payer to the payee. The payer generates a file that authorises the payee to initiate a transaction on the payer's behalf and transfers it to the payee offline. This file, which is the digital equivalent of an "IOU", can then be redeemed by the payees once they go online. This could be implemented for both register-based and value-based e-krona schemes, i.e. the register-based solution could also provide offline functionality.

Token-based primarily offline payments using secure elements

A truly value-based solution would be built on digital tokens that symbolise money and are stored locally in a secure element on a user's device or card. It would then be possible to transfer these tokens directly from one secure element to another without the devices necessarily connecting to the backend system. These secure elements have to exclude double-spending of tokens. In addition, an occasional online verification step could be included to increase security. This solution has the advantage of true anonymity and the possibility to perform consecutive offline payments. This concept would be very similar to payments with cash.

What we would like to add to the discussion

To prevent an unlimited outflow of e-kronas to foreign countries, Riksbank may wish to prohibit undeclared transfers to foreign countries and the use of e-kronas in those countries above a certain limit (as is currently the case for cash). With a register-based solution, this can be easily implemented as all transactions and participants are traceable. A value-based solution would require an additional means of control. The easiest approach would be to limit the amount of money that can be held in a wallet and the amount of wallets that can be stored on a device.

Conclusion

Riksbank in Sweden is considering a giant and very innovative step towards a new form of money and payment that would make digital central bank money available to the general public. This e-krona should give citizens access to risk-free money with the additional benefit of everyday convenience. We are convinced that user-friendly and very flexible authentication and app security solutions are a compelling proposition to deliver on this mission, providing innovative, highly secure and highly flexible consumer experience.

We are convinced that a register-based solution has the higher potential compared to a value-based system and recommend that Riksbank considers a value-based solution built on shadow accounts where wallet balances are stored in a database. This offers significant synergy benefits for both the consumers and the merchants' payment infrastructure.