Fidesmo wishes to contribute to the e-krona project with our technology and as an advisor with deep knowledge and understanding on security issues concerning secure elements. We propose, no matter what solution Riksbanken decides to chose; Fidesmo to integrate the e-krona to securely store it on wearables or cards for the public.

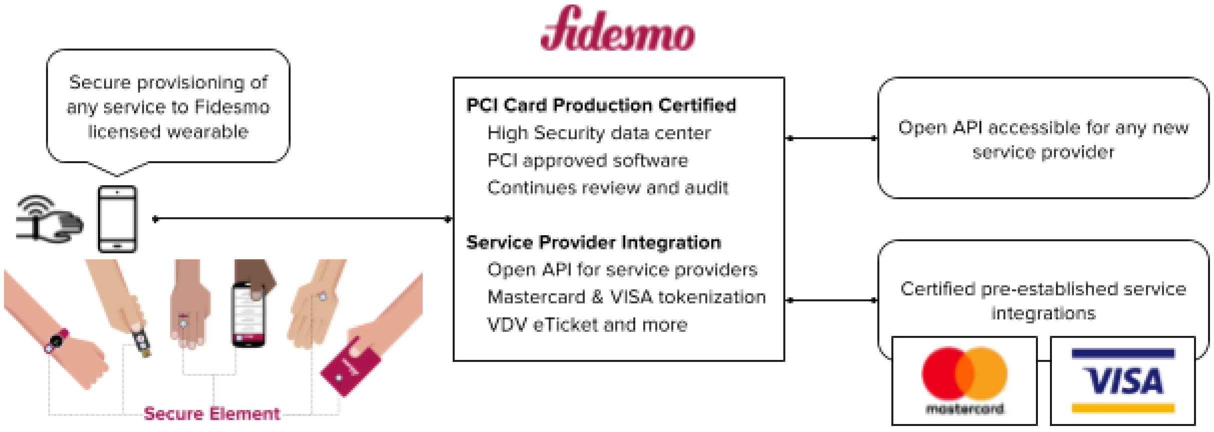
Introduction

A secure element is a mature technology used in the payment industry today. However, the technology lacks the flexibility of smartphone applications. Fidesmo has built the infrastructure required to remotely provision secure elements with different services making it possible to add "applications" after devices leave the factory similar to smartphones. Cards, watches, wristbands and other wearables, with a Fidesmo enabled secure element, fulfill the payment card industry's certification requirements and can be used to store payment card data for contactless payments. The same infrastructure can be used to secure the e-krona and to distribute the e-krona functionality to devices already in the hands of the consumer.

Fidesmo - the company

Fidesmo is a company that performs secure remote provisioning of secure elements. In most cases today, the secure element is provisioned at a factory (a process commonly referred to as *personalisation*) and then sent out to the customer. This prevents the end user from adding services to the secure element after they have received it. The Fidesmo platform enables end users to use a smartphone or tablet to add new services to their secure element device, allowing secure remote service provisioning to passive and active devices with embedded secure elements.

The Fidesmo solution is manufacturer agnostic and can work with several different types of secure elements, the only requirement is that the secure element has passed the certification process for security and functionality. Therefore; "off the shelf" secure elements from companies such as NXP[1], Gemalto[2] or ST-Electronics[3] can be personalized to work in the Fidesmo ecosystem.


fidesmo
Secure provisioning of any service to Fidesmo licensed wearable
Secure Element
PCI Card Production Certified
High Security data center
PCI approved software
Continues review and audit
Service Provider Integration
Open API for service providers
Mastercard & VISA tokenization
VDV eTicket and more
Open API accessible for any new service provider
Certified pre-established service integrations
mastercard
VISA

[1] "Security Controller ICs|NXP - NXP Semiconductors." https://www.nxp.com/products/identification-and-security/security-controller-ics:MC_71108.
[2] "Embedded SIM, eSE for consumer electronics: IoT ... - Gemalto." http://www.gemalto.com/iot/consumer-electronics/embedded-secure-element.
[3] "Secure Hardware Platforms - STMicroelectronics." http://www.st.com/en/secure-mcus/secure-hardware-platforms.html.

The Fidesmo platform is integrated with other companies that provision their services onto the secure element, often by securely authenticating the end user in the same process. Today there are already ongoing projects or finished integrations with several service providers. This includes Mastercard and VISA where the secure element is used to store a payment card token so users can pay via contactless with a Fidesmo enabled wearable, but also public transport tickets, access cards for buildings and Bitcoin wallets.

Due to Mastercard and VISA integrations, the Fidesmo solution is PCI-DSS[4] certified for the handling of payment card data and the software follows strict security requirements that are audited on a yearly basis. The solution also requires hardware that has been EMVco certified and fulfills the payment industry's security standards. Also, since sensitive information is provisioned into secure elements the entire Fidesmo solution is PCI - Card production[5] certified which has even stricter security requirements and requires that the services run in a Fidesmo managed high security zone, making the Fidesmo solution compliant for remote provisioning of payment tokens.

Fidesmo was selected by NyTeknik and Affärsvärlden as one of the hottest new technology companies in Sweden[6] for 2017. Also this year, Vinnova has financed a project with Fidesmo and Triwa[7] to bring tech and fashion together. Fidesmo is owned by the founders, employees and external investors, of which 82an Invest AB is the largest. 82an Invest AB is in turn owned by FAM, Karl-Johan Persson and Stefan Krook.

E-Krona security

Regardless if the e-krona system is registry or value based it needs a high level of security to prevent fraud and theft. This level of security can only be achieved with a secure element that acts as a secure storage of the identifier in the case of a registry based system, and in the case of a value system, the e-krona itself. Secure elements is a mature technology that today is already used in mobile SIM cards and payment cards. However, not all smartphones and almost no feature phones have a secure element - they instead use software called Host Card Emulation (HCE) to simulate the secure element without the security features.

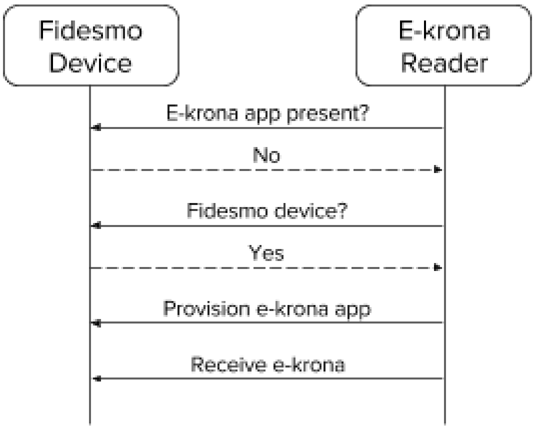
The weaker security of HCE[8] compared to a physical secure element limits their usage and increases the risk for any e-krona implementation that relies on HCE. While HCE solutions often use secure storage in the cloud the problem is just moved since secure authentication of the application is then required. This should ideally be a secure element but instead with device identifiers that can be manipulated. Cloning and stealing of HCE payment information has been demonstrated[9] with real world practical demos at security conferences showing how software protective measures can be circumvented for wide ranging fraud.

[4] "PCI Security - Official PCI Security Standards Council Site - Verify PCI ...." https://www.pcisecuritystandards.org/pci_security/.
[5] "PCI Card Production and - PCI Security Standards Council." https://www.pcisecuritystandards.org/documents/PCI_Card_Production_Physical_Security_Requirements_v2_Nov2016.pdf.
[6] "Fidesmo: Smarta chip fixar kortlös vardag | Ny Teknik." 4 Apr. 2017, https://www.nyteknik.se/startup/33-listan/fidesmo-smarta-chip-fixar-kortlos-vardag-6838534.
[7] "TRIWA | Buy watches, bracelets and sunglasses designed in ...." https://www.triwa.com/global/.
[8] Pardis Pourghomi, Pierre E Abi-Char, and Gheorghita Ghinea. Towards a mobile payment market: A comparative analysis of host card emulation and secure element. International Journal of Computer Science and Information Security, 13(12):156, 2015.
[9] HITBSecConf2017 - Amsterdam - Can't Touch This: Cloning Any Android HCE Contactless Card

Fidesmo’s contributions

The main issue with a secure element solution is that it is hard to change or add services to the secure element after it has left the factory. This limits their use and increases the cost since secure elements need to be bought for a specific use case instead of general use. Fidesmo enabled devices contain general use secure elements that can be remotely provisioned by the end user, allowing them to add the services they want. If the e-krona solution integrates with the Fidesmo solution, then end users could add their e-krona to their Fidesmo enabled wearables, increasing the e-krona exposure and making it easier for users to use the new e-krona.

A common problem for wireless NFC communication is network collision. If several NFC cards and devices are presented to a reader there is a race condition and network noise that interfere with the communication, which often results in the wrong chip establishing a connection or the reader rejecting all communication attempts. This is a common problem today since more and more cards are NFC enabled forcing users to take out the correct card from the wallet rather than putting the whole wallet on the reader. A Fidesmo enabled device or card would, due to the remote provisioning, have several services installed on the same card, allowing the user to have only one card or wearable in their possession and therefore not cause network collision among the different cards. The Fidesmo enabled chip would then present the correct applet to the reader according to its requirement. This allows e-krona to be present on the same card or wearable as public transport tickets and other services, making it more likely that users will take the e-krona with them as well as use it.



An e-krona solution that is integrated with Fidesmo can use the existing infrastructure to be remotely provisioned into any Fidesmo enabled device, allowing e-krona to be present in wristbands, watches, rings and other wearables. At the same time, the Fidesmo infrastructure and secure elements are certified for the payment card industry, fulfilling the requirements necessary for a financial system. Moreover, the default e-krona card could be a Fidesmo card that allows the end user to add more services to the e-krona card and therefore making it more likely that the e-krona will be a success.

With a Fidesmo integrated e-krona any Fidesmo card can be used to store the e-krona without any registration or extra action required by the end users. For a registry or value based e-krona, Fidesmo can develop the secure element applet to store the identifier or the e-krona itself on a Fidesmo card, making it possible for users to receive their change in e-krona format onto any Fidesmo enabled device they might have with them.

Fidesmo is a company working with contactless communication, authentication, payments and secure elements. We have extensive experience in these fields and even though we do not have an e-krona solution we would like to be part of any security consulting for the solution and in the future provide an authenticator or secure storage for the e-krona.