SAFEPAY

SafePay Systems Ltd.

THE FUTURE OF eSIM/iSIM

CAN OEMs LEARN FROM THE MISTAKES OF THE MOBILE OPERATORS?

Andras Vilmos, Managing Director, SafePay Systems Ltd.

The question in the title refers to the use of chip cards – eSIM, iSIM, embedded secure element - in smartphones and smartwatches for general security purposes.

January 2023

https://www.safepaysys.com/

Short Summary

- We have about 7bn smart communication devices (smartphones, smartwatches) on the market with at least one chip card (diverse types of SIMs and embedded secure element) inside.

- These chip cards are suitable for securely storing sensitive data, digital keys, documents (IDs) even applications.

- A technical specification was prepared by the GSMA, on how to manage secure applications (SAM) in the chip cards (eUICC) of smartphones.

- There is a new regulation in Europe, the Digital Markets Act (DMA), to be complied with by March 2024 at the latest, which opens up the secure elements in the mobile devices for 3rd party (service provider) use.

- **We "just" need a new logistical concept (e.g. the consumer-centric model) and an associated business model to let the chip cards in smart communication devices be used for secure applications and services.**

- Using the secure elements in the smartphones, smartwatches would (will) be a game changer in protecting our private lives and businesses.

- It seems that this game is over for the mobile operators, but we do not know yet whether OEMs will make better use of the valuable capabilities of the chips inside the smartphones. By all means, they are better positioned, and the necessary conditions are more favorable.

There are signs that the secure element(s) in the smartphones could - in the not-very-distant future - be used by any of us as secure storage of sensitive information, digital keys, and even applications. This would be a transformative change in securing our businesses and private lives.

Let’s assess the status of the necessary underlying conditions: **regulatory environment, technology maturity, market forces, business model, and motivation of key stakeholders.**

Regulatory Environment

There is a significant new development in the regulatory framework, at least in Europe.

“The European Parliament has adopted the Digital Markets Act (DMA) that will oblige Apple, Google and other “gatekeeper” technology companies to allow app developers and third-party service providers access to device functionalities “such as near-field communication technology, secure elements and processors, authentication mechanisms and the software used to operate those technologies”.[1]

DMA will move into its crucial implementation phase and start to be applied as of 2 May 2023. Gatekeepers will have to comply with the requirements in the DMA, at the latest by 6 March 2024.

DMA paves the way for the flexible use of the secure elements. The big question is whether other regions of the world will follow suit, establishing the conditions for harmonized regulations and uniform operating structures, which could greatly contribute to the penetration of secure mobile services.

However, to fully leverage the potential created by the new regulation, an adequate ecosystem needs to be built. This may have the consequence of some further regulatory involvement.

[1] https://www.nfcw.com/2022/07/07/377870/european-parliament-passes-law-that-requires-apple-to-open-up-its-nfc-chip/

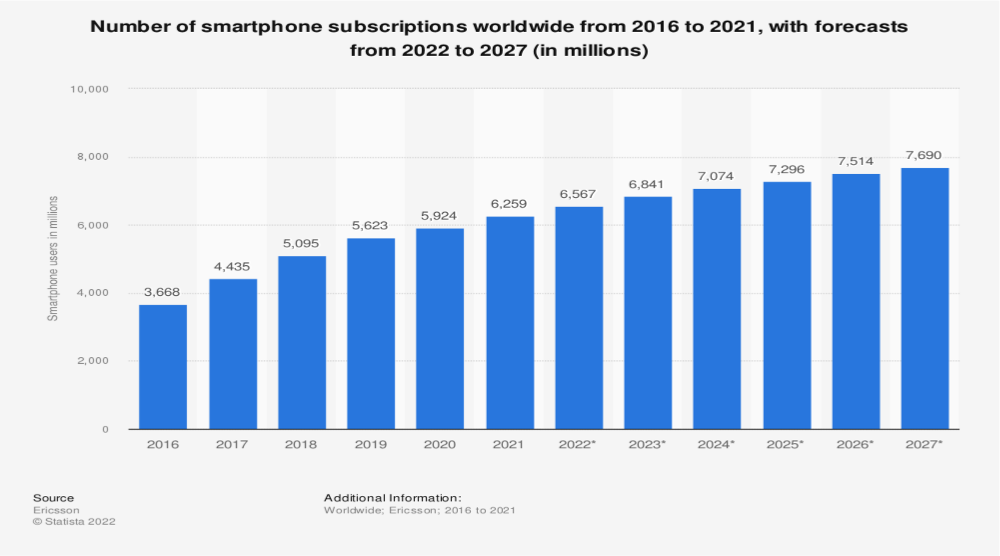
Technology

Secure elements

There are more types of secure elements – chip cards – in the smartphones than ever before. The removable SIMs (UICC) in various form factors, the eSIM and iSIM, as well as the embedded secure elements without the SIM functionality. All these chip cards could theoretically be used as secure storage devices.

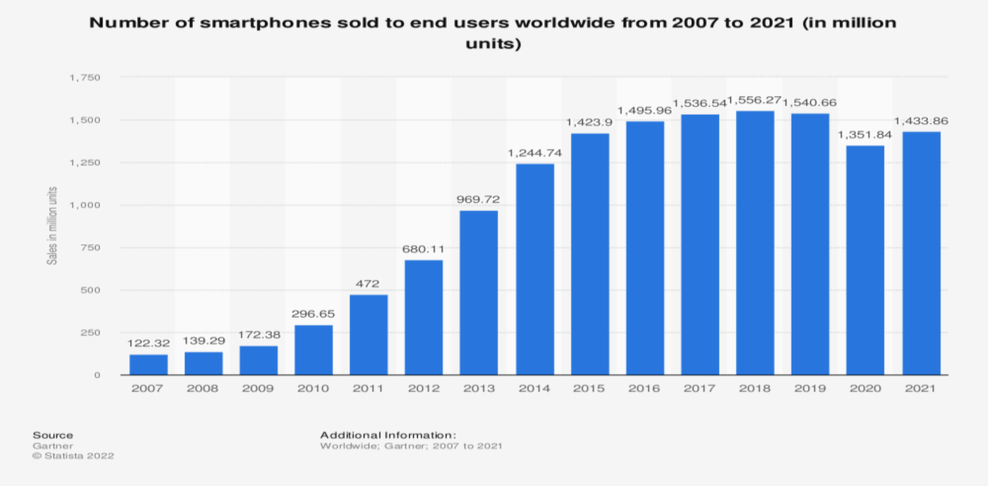
Smart phones

The availability of the necessary communication devices has greatly improved over the past years. There are almost 7bn smartphone subscriptions worldwide[1], with annual smartphone deliveries of over 1.5bn annually, including the new type of personal devices, the smartwatches.[2] All these phones have at least one secure element inside, which could be utilized by secure applications.


Number of smartphone subscriptions worldwide from 2016 to 2021, with forecasts from 2022 to 2027 (in millions)

Source
Ericsson
© Statista 2022

Additional Information:
Worldwide; Ericsson; 2016 to 2021


Number of smartphones sold to end users worldwide from 2007 to 2021 (in million units)

Source
Gartner
© Statista 2022

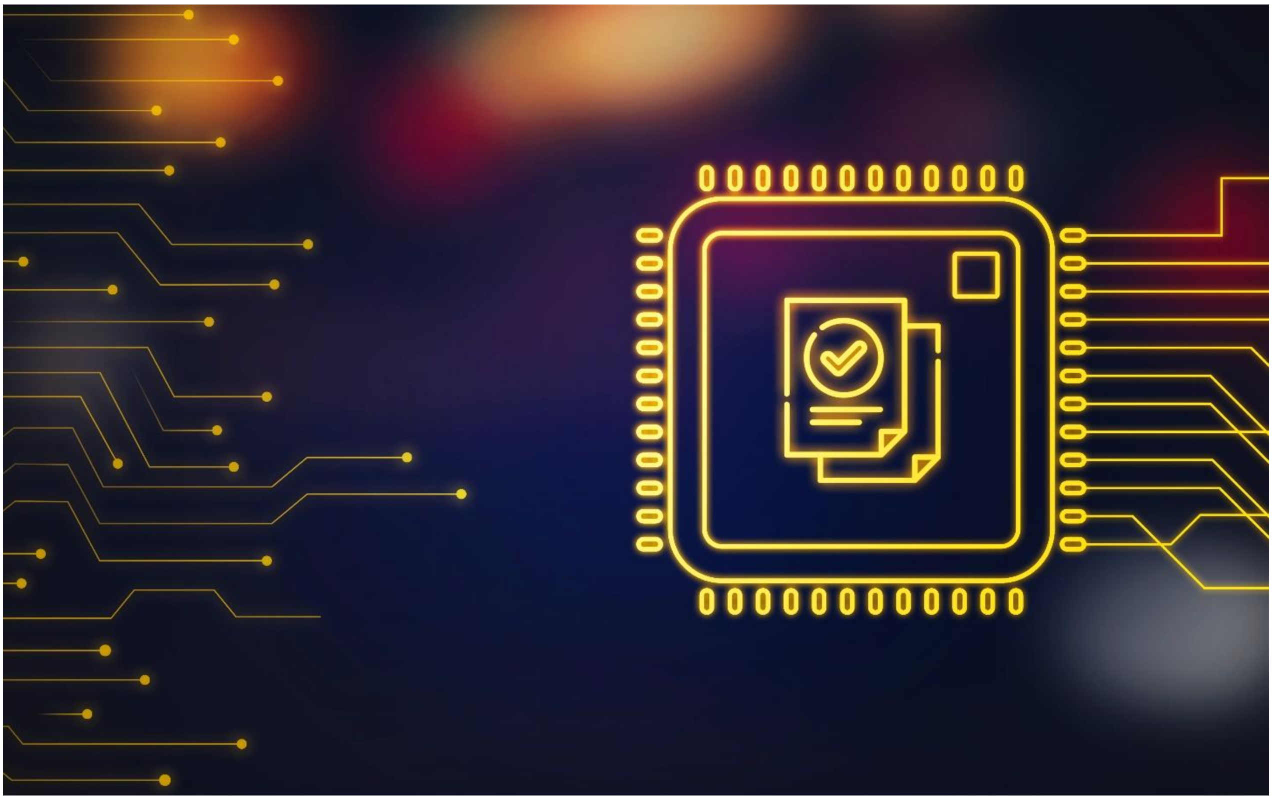
Additional Information:
Worldwide; Gartner; 2007 to 2021

NFC capability

In stark contrast to just a few years ago most smartphones and watches are also NFC capable. The secure applications/services could not only be used for securing online transactions but also for communication with various reader devices, POS terminals, gate readers, controllers, etc.

Application interoperability

It seems that we are getting closer to application interoperability as well. "The GSM Association has released a new requirement specification[2] focusing on Secured Applications for Mobile (SAM). This specification describes how cellular-connected devices (e.g. smartphones) may use secured applets within an eUICC (embedded universal integrated circuit card). Applets specified here can be managed by a service provider and are cooperating with applications running in the device itself."[3]



[2] https://www.gsma.com/newsroom/wp-content/uploads//SAM.01-v1.0.pdf

[3] https://blog.protocolbench.org/2021/06/gsma-published-requirements-for-secured-applications-for-mobile/

Logistics - Supply Chain

This is the most complicated part of the concept, requires the most work, because practically nothing has been achieved in this respect. It needs an attitude change from the owners (issuers) of the secure element; financial motivation for all stakeholders; and last but not least an integrated, fully automated supply chain. Without the right operating model, the DMA cannot achieve its desired effects either.

The consumer-centric model:
There are numerous use cases/services which could use the chip cards inside the smartphones. Every user needs a different secure service portfolio. Selection and installation of the secure applications should have the same user-friendly process and customer experience as regular mobile apps have, when installed from the various app stores.

This requirement has multiple consequences:

- There must be a known, formal set of standards/specifications which the secure applications must satisfy to be loadable to the chip cards inside the mobile phones. However, once these requirements are met and there is available storage capacity then the installation of the new services cannot be denied;
- There should not be any differentiation made between secure applications, and it should be the user/owner of the smartphone, smartwatch, who decides which applications get loaded into the chip;
- Allocation of the chip storage must be seamless and real-time, and the complex application loading, installation, and configuration process must be performed in the background, transparently for the user.

Application distribution/delivery
Service providers also expect efficient, transparent procedures.
Real-time, seamless application installation assumes that there is information about space availability on the chip card; and there is an architecture which can execute the over-the-air delivery of the specific application to the user's specific chip card.

There will be a space allocation issue, a key management issue, an application versioning issue, an application delivery issue, and an application personalization issue.
To establish this supply chain in an open, transparent, interoperable way, where any certified secure application, can be installed on any type of secure element, in any module of smartphone/smartwatch with whatever type of operating system, is the most difficult

challenge of this whole "secure application on the SIM concept". But it is manageable, needs industry consent and correct specification. (Do not think that a simple Trusted Service Manager – TSM – will solve the problem of an open ecosystem!)

As far as I know, no one is working now on such an open logistical/technical model, though this is the beginning and the end of the whole story. (In 2012 – not exactly yesterday – an EU project, StoLPaN, submitted such an open concept to Global Platform which could make sense to revisit.) The challenge is not only the complexity of the model but also the many actors involved from multiple industries and sectors, all having their specific, frequently conflicting motivations.

Application operation

Secure applications may need to be managed during their operation as well. They may need to be updated, may need new keys, new data, etc. These functions could be performed in-house by the service providers with a relatively simple architecture (anyone managing smart cards in their legacy service could do this) or could be made available as 3rd party, outsourced service. The good news is that all the necessary functions and communication are already specified by Global Platform, so this hurdle is relatively easy to take.

Business Model

In this complex ecosystem I just consider the key stakeholders, who must transact with each other, in an ad hoc manner, potentially also without long term agreements and without bilaterally pre-negotiated financial conditions. Such ad hoc business scenarios between potentially unknown partners may be new in the trusted world of chip cards, but it is quite ordinary in many other online business relations.

The key actors, whose financial requirements need to be satisfied are the

- end users;
- service providers;
- secure element issuers (owners of the secure element).

Others involved in the transactions are working on behalf of one of these three parties.

The axioms, which seem to be obvious but have been questioned in the past:

- Security has value that must be paid for;
- Service providers must generate revenues for the services they provide;
- Provisioning secure storage capacity costs money which needs to be recovered from revenues.

The point of the story is that consumers will need to pay for secure mobile services. This is not an uncommon business model even in the telecom sector as premium/paid apps are widely used. (18% of apps in app stores are to be paid for and related revenues are reaching 18bn USD in 2022.[4]) The secure mobile apps may cost somewhat more than basic ones, but the principles are the same.

[4] https://www.statista.com/statistics/263797/number-of-applications-for-mobile-phones/

Market and Demand

Mobile payment

Mobile payment became mainstream already today with Google Pay, Apple Pay, Samsung Pay, Ali Pay, PayPal, etc. Emarketer expects 1.31 billion people to use mobile payment this year. In 2021 almost 30% of POS payments have been made with mobile wallets. Most mobile payment transactions are presently performed using one of the large wallets, which model will undoubtedly change. This is the primary reason why the DMA is forcing gatekeepers to allow access to their secure elements. However, the overall pie should become larger which may provide some/adequate compensation for the wallet operators.

Mobile ticketing

Contactless transport ticketing solutions are proliferating all over the world. The technology has been implemented in numerous large cities worldwide and the penetration continues. Several million people use it day after day and its expected value is forecasted to exceed US 10Bn this year. However, the “rising concerns of security and safety risks associated with the usage of this type of ticketing system may hinder the global contactless ticketing market growth. When credentials are stored in mobile devices that lack security, hackers can try to break in the system and steal the confidential data.”[5] Using the SIMs inside the mobile devices for storing the tickets would give an additional boost to the growth of this sector.

The rising demand for smart ticketing from sports, entertainment, and tourism sector is another opportunity for using secure smart devices in the ticketing sector. Buying tickets online, having the tickets delivered into the smartphone, storing it securely in a secure element and then presenting the ticket upon entry with a touch of the mobile device is an unbeatable security and convenience combo for a huge mass market.

[5] https://www.futuremarketinsights.com/reports/contactless-ticketing-market

Digital ID

Digital ID, or better said mobile ID, more accurately various mobile IDs – national IDs, passports, driving licenses, boarding cards, etc. – is a relatively new phenomenon, but with a global reach, great legislative support, and a vast prospective market.

The European Commission has a digital ID program, with the objective of all European citizens having one in a mobile wallet. The ICAO has prepared the specification of its Digital Travel Credential (DTC) to standardise the issuance of travel credentials in digital format. Based on the ICAO DTC principles, IATA One ID is about to become the main digital identity standard within the aviation industry. In the US, the American Association of Motor Vehicle Administrators (AAMVA) is leading the Mobile Driving License (mDL) efforts in North America and works closely with its counterparts across the world to ensure global interoperability and acceptance. Also, the World Bank has a related initiative, and many countries have already introduced their digital IDs or are about to do so. There are alternative approaches to storing these IDs on the chip in the mobile phones, but none can be as secure, as convenient, and most probably as efficient and affordable like this technology.

Identification and Access Management (IAM)

IAM is another domain where chip cards have long been used and which could be revolutionized with introducing the secure mobile application technology.

FIDO (Fast ID Online) is based on free and open standards from the FIDO Alliance for secure online authentication. During registration with an online service, the user's client device (in the secure mobile scenario this will be the secure element in the smartphone) creates a new key pair. It retains the private key and registers the public key with the online service. Authentication is done by the client device proving possession of the private key to the service by signing a challenge. FIDO is supported by all major browsers.

Cold wallets are used in the crypto world to store larger amounts of crypto currency offline, as a protection of the funds. The solution is really secure, but rather user hostile. The secure mobile architecture would be a great alternative providing the secure storage and the always on capability for the wallet application.

Front-end Access Management (FEAM) is a new type of authentication and authorisation technology, which combines the best features of FIDO and OAuth. The chip card in the mobile could be used for authenticating the user, authorizing the transactions, and generating the web token to be used to receive access to the protected resources. The technology can be used for both online and offline access.

Bring Your Own Device (BYOD) received real meaning and importance with widespread remote work practices. The integrated secure elements could well be used for securely authenticating the users' communication devices thus substantially improving enterprise security.

The above list contains only a handful of potential use-cases which could well leverage the potential of secure elements inside the communication devices.

In summary, we can determine that most conditions, except the integrated supply chain and the associated business model, are ready for the breakthrough change of using the chip cards inside the smartphones and smartwatches for our personal security purposes.

Knowing all these facts, let’s try to answer the question in the title “CAN OEMs LEARN FROM THE MISTAKES OF THE MOBILE OPERATORS?” in utilizing the secure elements in the smart communication devices.

There are about 7bn smart communication devices with SIM cards inside on the market. Many of them already have a second embedded secure element. Many smartwatches have integrated SIM cards. New smartphones will come with eSIMs and iSIMs, for a while co-existing with the regular removable SIMs, but soon replacing them. While the removable SIMs are owned by the MNOs, the eSIMs, and iSIMs will most probably be controlled by the device manufacturers, OEMs.

It all seems that due to these technical trends, Mobile Network Operators (MNO) have eventually lost their opportunity to leverage the security capabilities of the SIM cards. (Removable SIMs will most probably disappear before the ecosystem of secure mobile services will become mainstream.) MNOs failed to capitalize on the opportunity, failed to establish the additional revenue stream, as well as the potential to provide value-added services for their customers.

For sure OEMs are better positioned to leverage the secure elements of the smart devices. MNOs had the inherent fear of using the SIM for anything else than their own telco purposes. They wanted to control everything and wanted to control it expensively. This prevented any progress in this regard in an otherwise fairly flexible and innovative group of companies. The OEMs do not have this panic. For them, the secure element could be considered as a piece of hardware, which under the right conditions could be treated just as a simple commodity and could generate sizeable revenues.

The overall environment is also much more welcoming than it was just a few years ago. The technical requirements have developed well in the past years, and the necessary conditions are readily available now. The potential market grew a lot, and it became quite substantial, with legacy services growing and new ones proliferating quickly. Security has never been as hot a topic as it is today, which shows that there should be real demand for convenient and user-friendly solutions. Even the regulatory requirements could support better utilisation of the secure elements.

Everything points into the direction that this time we could be more successful. The one remaining important challenge is the specification of the overall supply chain. This would need the cooperation of numerous sectors and even more partners, who may otherwise never talk to each other.
Google made the first move into the right direction with forming the "Android Ready SE Alliance" [6]. As Google phrases it: this is a collaboration between Google and Secure Element (SE) vendors. This is a promising step though much broader industry participation would be necessary, involving also the OEMs and service providers.

Let's hope that this time common sense prevails, the OEMs will better understand the market requirements, and we all will benefit from using the valuable property of secure elements in our smartphones and smartwatches.

[6] https://developers.google.com/android/security/android-ready-se