EUROSMART
The Voice of the Digital Security Industry

GSMA SAM solution: opportunities and challenges for mobile identity

Introduction

In the context of the proposal for a European Digital Identity framework[1], Eurosmart would like to give its views on the Secure Application for Mobile (SAM) technology specified by GSMA. SAM technology is multipurpose and can be used for a wide range of use cases. It has capabilities to manage secure applications such as banking, transport, health, identity etc.

Secure Mobile identity is a specific use case of this technology, making SAM a potential candidate for the technical architecture of the European mobile identity. This document will focus on this particular use case.

First, Eurosmart would like to state some general principles on mobile identity. Such principles need to be kept in mind when considering any mobile identity solutions. Secondly, Eurosmart will provide recommendations for a successful implementation of the GSMA SAM solution.

GSMA SAM technology requirements are the foundation that will be used to create technical specifications. Given that GSMA is still defining SAM, Eurosmart will limit itself to giving some key recommendations before commenting in more detail once a final version of the specifications is released.

Core principles for mobile identity

In this section, Eurosmart provides -on two topics- some general principles that should apply in the context of mobile identity. Both topics are crucial for Europe's sovereignty.

Member States should remain in control of digital identity issuance

Historically, States have provided their citizens with a legal identity giving them access to rights and justice so that they can protect their rights. It led them to organise the issuance of legal identities through the management of citizens' life events (e.g. register of birth, register of death) and the issuance of an identity document (checking that the applicant, the claimed legal identity and the identity document recipient are the same) so that citizens could prove

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (SEC(2021) 228 final) - (SWD(2021) 124 final) - (SWD(2021) 125 final).

their legal identities. As such, the provision of identity to citizens has been a sovereign power for centuries, exercised mainly by the State.

It is key to understand the importance of a strong link between a proof of identity presented by a citizen and the legal identity of this citizen. Only the latter grants a citizen with rights and obligations, but the proof of identity is the only thing a citizen can provide to state his/her identity. Therefore, the proof of identity needs to be related to a legal identity in a very reliable manner. For these reasons, EU Member States shall remain in control of issuance of digital identity proofs and credentials. If private actors are involved, they shall be accredited and supervised by the EU Member States.

In addition, the EU regulatory framework shall prescribe a separation of functional layers to avoid market concentration. Gatekeepers, such as manufacturers of connected devices (e.g. smartphones, watches, tablets, cars), which provide users access to the internet (through a search engine, device, application stores etc.), shall neither secure their digital identities nor be identity providers. If so, they would also control the access of services to users, as they would become inescapable to verify users' digital identities. This is crucial to ensure fair competition and avoid having a commercial/non-governmental entity locking the entire digital value chain.

Take into account the conditions laid down by application stores

Digital identity on mobile will surely rely on applications and application stores. These are elements to take into account. Measures need to be taken to ensure that European citizens can always access and use their mobile identities if they are entitled to do so by European laws. It should not be possible for the owner of an application store to unilaterally decide whether European citizens can still access or use their mobile identities, for instance, as a consequence of a geopolitical situation (export ban).

Eurosmart has performed a legal analysis of the terms of use and the standard developer agreements for the main providers of application stores. Our findings show that developers (i.e. entity providing applications to be loaded on connected devices) are bound by their agreements with the providers of applications stores and must comply with non-EU export control rules. In addition, it appears that the main providers of application stores enjoy a sort of discretionary right to remove an application from their application stores. Developers are also subject to non-EU courts and laws in case of legal claims.

From a user perspective, the terms of use mandate to create an account with the provider of applications stores. The terms of use also allow such providers to re-use application/user data for commercial purposes and give them the possibility to deactivate user's access to the store in some cases.

SAM technology: recommendations

In this section, Eurosmart highlights the technical conditions that should be met by SAM technology so that it can be used for the European mobile identity.

What is SAM technology?

SAM technology relies on the eUICC[2] technology, which is a secure area available on most connected devices. The eUICC is a tamper-resistant secure element based on secure hardware, which is security certified at a high level. This is why sensitive data can be securely stored in the eUICC.

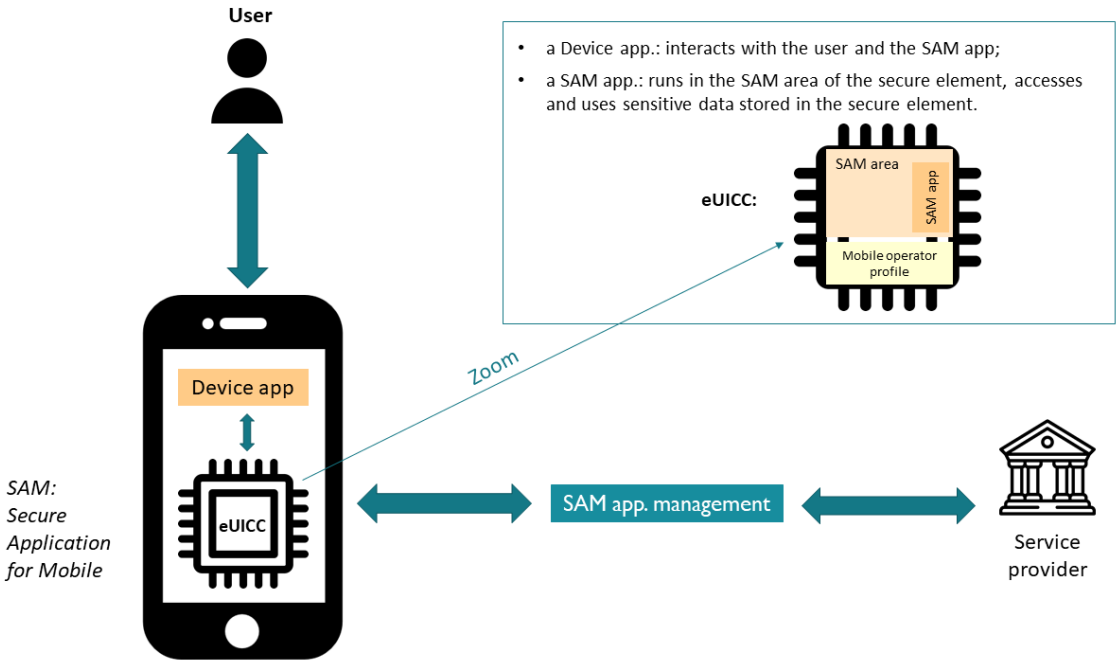
The eUICC usually takes the shape of a chip embedded, integrated or removable in connected devices. The eUICC is progressively replacing the removable SIM card – used so that a device can connect to a mobile network – and allows the user to download a mobile operator profile on the eUICC instead of inserting a SIM card. The procedure is fully digital. It is worth noting here that the eUICC is provided by device manufacturers, whereas mobile operators provide the traditional SIM card.

SAM technology enhances the eUICC with a logical area (SAM area, also called SAM Security Domain) independent from any mobile operator/service provider eUICC profile. Therefore, should the user decide to change mobile operator, he/she could switch to a new mobile operator profile, and the content of the eUICC will be updated, **except this SAM area**. The user can also have multiple operator subscriptions, and the SAM area will remain whatever the number of operator profiles stored and activated.

The SAM applications and the sensitive user information they contain can hence be securely stored in the eUICC in an isolated way. The SAM applications and user credentials contained in the SAM area of the eUICC would not be changed. This immutable area could be used for the storage and secure execution of SAM applications (and the storage of corresponding credentials) bound to the user. It would not depend on the user being the customer of a given mobile operator (unlike applications in an eUICC profile). Therefore, the user can keep its SAM applications and corresponding credentials on the same device, even if he/she changes mobile subscription.

Please find below a picture that gives a simplified overview of the SAM technical architecture and its secure area.

[2] embedded Universal Integrated Circuit Card.



Note on the picture:

In the present picture, the service provider is responsible for (1) providing the SAM application and (2) providing the service to the user relying on the said SAM application. However, it will often be two separate roles:

- *The **application provider** in charge of developing the SAM application on behalf of the service provider. The development of the SAM application may be performed under the supervision of the service provider (e.g. security certification);*
- *The **service provider** per se in charge of providing the service to the user, relying on the said SAM application.*

A common example is the case of payment applications, where the payment scheme will provide the service to the user but will not develop the SAM application. Its development will be delegated to a third party, which will have to achieve a security certification of its SAM application.

Security aspects

Eurosmart strongly underlines the need to ensure the continuous security of SAM technology. This entails several considerations.

The security of SAM applications (and of the user's credentials they contain) -stored and running in the SAM area- relies on the security of the underlying eUICC hardware supporting SAM technology (e.g. crypto, memory management, isolation with the other part of the eUICC). Therefore, the eUICC hardware (or tamper-resistant element in a SoC) shall be security certified at least at Common Criteria level EAL4+AVA_VAN.5 to guarantee secure storage and execution of SAM applications. To comply with relevant EU legislation (e.g. eIDAS), the EUCC

scheme[3] shall be used for the security certification of the eUICC hardware supporting SAM technology. Moreover, as it is foreseeable that digital identity regulations will leverage the Cybersecurity Act[4] regarding security certification, this entails using the EUCC scheme for security certification of the eUICC hardware supporting SAM technology in the context of digital identity. However, for other use cases or another geographical context, alternate security certification schemes could be used.

Sensitive SAM applications (e.g. qualified electronic signature application or digital identity application reaching Level of Assurance "High" pursuant to eIDAS[5]) shall also be security certified. There are several ways of certifying the SAM applications depending on the use case. This usually implies composition with the underlying eUICC.

Eurosmart highlights that it is needed to define a protection profile for the eUICC supporting SAM technology in order to allow such security certification in composition. Eurosmart recommends preparing a protection profile for the eUICC supporting SAM technology. Furthermore, Eurosmart strongly recommends leveraging existing protection profiles. Based on an analysis of the relevant protection profiles, the most suitable one should be updated. Alternatively, if deemed useful, a new protection profile may be developed.

Additionally, Eurosmart would like to stress the importance of end-to-end security: security should be guaranteed from the eUICC supporting SAM technology to the corresponding provisioning server. The security of the latter shall not be forgotten as it plays a key role in the overall security of the infrastructure.

Also, pursuant to the EUCC Scheme, a security certificate has a limited lifetime, and, in case of a security breach, its validity may be withdrawn. However, as stated above, security certificates of SAM applications stored and running in the SAM area depend on the underlying eUICC supporting SAM technology. In case a security breach on the eUICC could not be patched, the eUICC would lose its certificate. Then, the SAM applications would also lose theirs, leading to major concerns for the user. For instance, if the eUICC supporting SAM technology loses its security certificate, the qualified electronic signature application (QSCD pursuant to eIDAS) running on it would not be able to generate a qualified electronic signature anymore having the same legal effect as a handwritten signature. Thus, the electronic signature of the user could not be considered reliable anymore, which would have a substantial impact when legally binding documents need to be signed.

It is crucial to maintain the required security certification of the underlying eUICC supporting SAM technology to enable citizens to use sensitive SAM applications (for which security certification is needed) and provide them with a smooth user experience. Keeping up the security of the eUICC over time is the responsibility of the manufacturer of the device (in relation to the manufacturer of the eUICC).

[3] The EUCC scheme is the first European cybersecurity certification scheme adopted pursuant to the Cybersecurity Act. It is the transposition of the existing SOG-IS MRA.
[4] Regulation (EU) No 2019/881.
[5] Regulation (EU) No 910/2014.

Key recommendations on security

- Require security certification of the eUICC hardware at Common Criteria level EAL4+AVA_VAN.5 at least.
- Require security certification of sensitive SAM applications.
- Leverage existing protection profiles for the security certification of SAM technology.
- Establish a process for device manufacturers to maintain the level of security certification of the hardware platform.

Trust model

In SAM technology, a root of trust is responsible for delivering authorisations to third parties willing to load a SAM application in the SAM area of the eUICC supporting SAM technology. This root of trust is hence the ultimate authority controlling the utilisation of the SAM area in the eUICC to install a particular SAM application. The owner of the root of trust is the entity that owns the eUICC (device manufacturers), and it is usually a private entity, sometimes a foreign one, that may be ruled by foreign laws.

In some cases, and in particular, for digital identity, SAM applications are intended to store and use identity credentials issued by a State. This may be problematic. A State may not agree to depend on a private entity, especially a foreign one, ruled by foreign law. It may be perceived by States as violating their sovereignty, and as such, it shall not be underestimated. It may have a deterrent effect on States for the adoption of SAM technology to deliver digital identity applications on mobile.

For digital identity use cases, Eurosmart recommends policymakers mandate the use of national roots of trust within SAM technology so that the management of identity applications (including the corresponding attributes) could be controlled by a national root of trust ruled by national laws. For example, in the future, it should be possible for Member States to download eID SAM applications independently from any device or company online application store. This echoes Eurosmart's comments on applications stores, as stated above.

Key recommendations on the trust model

- For digital identity use cases, mandate the use of national roots of trust.
- Member States should be in a position to control the management of the sovereign eID applications.
- Ensure that Member States can remain in control of the provisioning and management of national identity data.

Data protection

Eurosmart's views are that SAM technology should be fully in line with data protection principles, as enshrined in GDPR and the future ePrivacy Regulation.

First, user credentials should **not** be known by mobile operators or connected device manufacturers and even less re-used.

Secondly, it is essential to consider the circular approach, which is currently encouraged by the European Commission. There is already a large second-hand market for connected devices in Europe, and this will keep growing. We will also see better recycling of connected devices, including re-use of sub-elements, e.g. eUICC. This raises questions about the effectiveness of the factory reset. Can citizens be confident that their data is fully erased when they start a factory reset? This should be the case; otherwise, this would compromise both the uptake of SAM technology and the much-needed circular approach.

Therefore, Eurosmart calls for the security certification of the eUICC supporting SAM technology to also cover the secure erasure of SAM applications and user credentials in case a factory reset is performed. This shall be included in the protection profile to be prepared for the eUICC supporting SAM technology.

Key recommendations on data protection

- Forbid access and re-use of user national identity credentials.
- Extend the scope of the security certification of the eUICC supporting SAM technology to cover the secure erasure of SAM applications and user credentials in case of factory reset.

SAM actors and technology interoperability

SAM technology aims at allowing the development of an open ecosystem comprising several stakeholders:

- **The service provider (e.g. public transport authority, university…)** provides a service to the user (e.g. access to public transport, identification to access online courses), relying on a SAM application being stored and executed in the SAM area of the eUICC.
- **The entities in charge of providing (and developing) SAM applications**. These entities develop SAM applications on behalf of service providers willing to offer services to a user relying on the hardware security brought by the eUICC of his/her connected device.
- **The entities in charge of loading and managing SAM applications in the SAM area of the eUICC of connected devices (e.g. mobile operators, sectorial organisations) remotely.** These entities act on behalf of service providers willing to offer services to

the user, relying on the hardware security brought by the eUICC of his/her connected device.

- **The provider of the eUICC nested in the connected device of the user.** It may be the connected device manufacturer but could be different. A priori, there is no direct relation between the service provider and the provider of the eUICC.

In order to achieve successful deployment of SAM technology, as well as to avoid a lock-in phenomenon, interoperability is key.

From the perspective of service providers:

The interoperability between SAM applications and the eUICC is instrumental to ensure independence between entities providing SAM applications and the eUICC/connected device providers. In other words, it is important to guarantee that the service provider is not bound to the eUICC/connected device provider, and more precisely, is not locked in with proprietary technologies for the development of SAM applications. Standardisation is key in this respect, as it will provide interoperability and portability and prevent proprietary solutions. Eurosmart recommends prescribing interoperability and portability of SAM applications through the use of standardised technology.

The portability of SAM applications on the eUICC supporting SAM technology can be solved thanks to harmonised programming language, such as Java Card™, where SAM applications would be Java Card applets, ensuring they can be loaded and executed on any eUICC. Unfortunately, such a requirement is currently missing in the SAM document, which could hamper interoperability.

On top of this, interoperability of SAM applications encoding should be ensured. In that regard, test activities encompassing test specifications and events could be useful.

From the perspective of entities in charge of loading and managing remotely SAM applications in the SAM area of the eUICC:

The interoperability between the eUICC supporting SAM technology and the entity in charge of loading and managing SAM applications remotely may not be straightforward. Yet, it is instrumental for the success of SAM technology. Therefore, it is very important that technical specifications are also prepared to ensure the conformity of components over these interfaces. For example, the mechanisms defined by GlobalPlatform for loading and management of applications on secure elements could be considered in the scope of SAM technology. GlobalPlatform specifications for the loading and management of SAM applications could be referenced. In particular, SAM technology could leverage Secure Channel Protocols (SCP) defined by GlobalPlatform.

Reconciling security and portability of SAM applications:

In the case of sensitive SAM applications, requiring to be security certified, some specific issues arise, which have direct impacts on the overall portability. Usually, under the Common Criteria approach, it is a key challenge to reconcile the security and portability of SAM applications.

Pursuant to the composition methodology provided for by Common Criteria, the security certification of a SAM application is carried out in composition with the eUICC supporting the SAM technology. The evaluation centre (1) evaluates and analyses the SAM application, as well as (2) carries out vulnerability assessment (using penetration tests) of the SAM applet loaded and running in the eUICC supporting SAM technology. However, usually, as the developers of the eUICC supporting SAM technology and the SAM application may be different, the latter, as well as its evaluation centre, does not have access to the internal design of the eUICC supporting SAM technology to prepare and carry out the evaluation of the SAM application. This is for obvious reasons of protection of intellectual properties.

Therefore, the SAM application developer and its evaluation centre have to handle the eUICC supporting SAM technology as a "black box". In the current methodology, the developer of the eUICC supporting SAM technology provides recommendations to the SAM application developer so that its SAM application is secure (how to code SAM application). In addition, the evaluation centre, having carried out the security evaluation of the eUICC supporting SAM technology, provides the main findings to the evaluation centre of the SAM application.

The security certification of SAM applications according to the composition methodology defined by Common Criteria, unfortunately, entails some drawbacks:

- **The design of the SAM application is bound to a particular type of eUICC supporting SAM technology on which it is intended to be loaded and running**. In order to be security certified on a particular eUICC supporting SAM technology, the SAM application has to apply the development recommendations provided by the developer of the eUICC supporting SAM technology.
- **The developer of the SAM application depends on the developer of the eUICC supporting SAM technology**. In order to have its SAM application certified, the SAM application developer shall get the active support of the developer of the eUICC supporting SAM technology to get access to the development recommendations, but also so that its evaluation centre also gets access to the main findings of the security evaluation of the eUICC supporting SAM technology. In particular, it means that the developer of the eUICC supporting SAM technology may refuse or impose particular conditions.

Therefore, in the case of certification in the composition of SAM applications, these consequences restrict the portability of SAM applications:

- **SAM applications have to be designed for a specific eUICC supporting SAM technology**. As many versions of SAM applications as there are versions of eUICC supporting SAM technology are needed. Security considerations cause to break the universal portability brought by a standardised programming language (e.g. Java Card technology);
- **A formal agreement will have to be set between developers of SAM applications and developers of eUICC supporting SAM technology**. The latter may refuse to collaborate or impose particular conditions to collaborate (e.g. financial ones).

Thus, while a standardised programming language (e.g. Java Card) provides for a functional portability of SAM applications, the security certification should not be a step back for portability.

Eurosmart believes it is possible to reconcile both aspects (security and portability). The Common Criteria methodology under the SOG-IS agreement and the EUCC Scheme should be enhanced to allow security certification at the highest level (with component AVA_VAN.5) of SAM applications in composition with eUICC supporting SAM technology in a portable manner. It shall be possible to perform generic security certification of SAM applications for any suitable eUICC supporting SAM technology. This would solve the current issue where a Common Criteria security certificate obtained using composition methodology is bound to (1) a particular SAM application and (2) a particular eUICC supporting SAM technology.

Key recommendations on interoperability

- Prescribe interoperability and portability of SAM applications through the use of standardised technologies.
- Leverage existing standards and specifications, such as Java Card and GlobalPlatform's Secure Channel Protocols.
- To also make security certification of SAM applications portable, the Common Criteria composition model should be enhanced.
- Trust the Common Criteria methodology to provide the security certification of eID SAM applications.

Governance for SAM-based mobile identity

GSMA SAM does not address the subject of governance since GSMA SAM's deliverables are only technical. Eurosmart understands that this is not within the remit of GSMA to tackle governance issues.

However, if the SAM solution is used for mobile identity, governance issues cannot be left untackled. Eurosmart believes that the European Commission and the Member States should start working on a governance model in the context of the SAM solution applied to digital identity -in accordance with the provisions of European legislation on digital identity (e.g. eIDAS). In Eurosmart's view, this model should clearly define the roles and responsibilities of the actors from the mobile identity ecosystem. This governance model needs to be flexible enough to adapt to future technological changes and different business models.

In addition, the Commission and the Member States should translate this model into a legislative framework to avoid competition distortion. It is important for this governance model to allow the SAM solution to be an open ecosystem that enables players to use it independently from individual private stakeholders (e.g. mobile operators, sectorial organisations, device manufacturers, eUICC manufacturers etc.). Therefore, a regulatory framework defined at the EU level is much needed. This could be a complement to the revision of the eIDAS Regulation.

Key recommendations on governance

- Define a governance model in the context of the SAM solution applied to digital identity.
- Translate this model into an EU legislative framework.

Conclusions

Eurosmart strongly believes in the potential of SAM solution for mobile identity. In this document, Eurosmart makes recommendations for a successful deployment. This work was designed as an input for further discussion with the European Commission, Member States and other interested stakeholders.

The importance of this topic calls for setting up a working group on mobile identity. Should the European Commission consider setting up such a group, Eurosmart would happily participate in providing its insights. In particular, Eurosmart would gladly (1) lead the creation of a SAM Protection Profile covering the SAM features, preferably relying on existing ones, and (2) actively contribute to an enhancement of the Common Criteria composition model to provide for security certification of SAM applications at the highest level.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on a chip, High-Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics, Synopsys, Thales**, **Tiempo Secure, TrustCB, Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Contact@eurosmart.com