Federal Office
for Information Security

Position Paper

SAM – Secured Applications for Mobile

Executive Summary

The widespread use of smartphones and digital mobile services has revolutionized all parts of the society. Along with the increased usage there is a growing dependence on secure digital identities in this context. The embedded SIM (eSIM) as a hardware security trust anchor serves a critical role in ensuring security of identity information. It is a tamper-resistant component embedded in many smartphones that securely stores and manages authentication credentials and encryption keys.

Within the EUDI wallet initiative, the goal of the BSI is to establish a sovereign and decentralised eID-System based on existing highly secure hardware-based solutions to achieve cybersecurity for the society and economy independently from third party concerns. The promising Secured Applications for Mobile (SAM) initiative provides a secure platform on eSIM hardware (see Figure 1) for use cases not only belonging to mobile telecommunications, e.g. electronic identities (eID). The project is currently in the process of standardisation by GSMA, GlobalPlatform and other organisations, which will ensure interoperability, security, and privacy across systems of different manufacturers. SAM has the potential to become a key component for the sovereignty of the EUDI wallet and their secure and decentralized eID-Systems.

Various global players from industry and standardization are supporting this evolution towards a modern eSIM platform. Notably to mention the position of Eurosmart regarding SAM [Eusm-SAM] and Wallet-Certification [Eusm-Wallet], the GSMA approach to secure IoT services [GSMA-IoT] and the Trusted Connectivity Alliance position on SAM [TCA-SAM]. This position paper presents the current view of the BSI on the Secured Applications for Mobile technology within the scope of electronic identities for mobile devices.

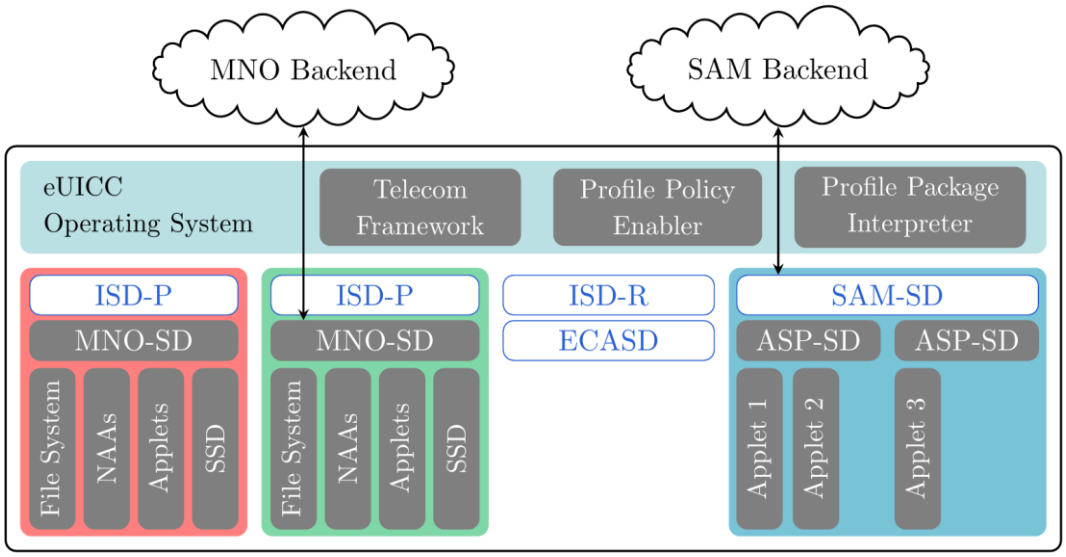

Figure 1: In addition to the functionality required for telecommunication services, a SAM-enabled eSIM provides an additional security domain (SD) for third-party applications. Schematic adapted from [SGP.21].

eID Use Case

Electronic identities are a key enabler for governmental and commercial digital services. Requirements for eIDs, with regard to security and privacy, are grouped in three levels of assurance (LoA) ranking from low to high [eIDAS-Reg]. Hereby, the highest level can usually only be achieved if dedicated security chips are utilized to store and use cryptographic key material and the user's identity data. Consequently, eID schemes aiming for LoA high demand for secure and tamper-proof hardware elements as for instance an eSIM as a trust anchor in the user's mobile device in order to achieve the appropriate level of security. In addition to security and privacy of individuals, the digital sovereignty of EU member states is an important aspect of governmental eID solutions. This is particularly relevant for applications like the EU Digital Identity Wallet (EUDI-Wallet). As a central aspect of the future European digitization strategy, all EU member states will offer a wallet solution to their citizens for digital participation (eIDAS 2.0). Besides governmental applications, third party providers from the private sector also have content in need of protection. Business areas such as mobile payment, transport ticketing, secure IoT Services or similar use cases have a legitimate interest in hardware security on mobile platforms, too.

eSIM Evolution

Securing critical information in mobile devices is key to ensure the secure usage for citizens and safe businesses. Starting from the beginning of the commercial introduction of the Global System for Mobile Communications (GSM) in the early 1990s, mobile network operators (MNO) have relied on the usage of a dedicated tamper-proof hardware element called Subscriber Identity Module (SIM). The SIM isolates cryptographic security functions and algorithms as well as related secret keys used for authentication and key agreement for every individual mobile device. The tampering or retrieval of credentials is prevented by countermeasures at architectural and hardware level.

With the establishment of embedded SIM, the next stage of the development of dedicated hardware security elements in mobile devices will be accomplished. As a trust anchor, the eSIM is security evaluated and Common Criteria (CC) certified on a high assurance level. Personalization of the subscription data is realized over the air in the field, triggered by the user of the mobile device. The personalization process uses the Remote SIM Provisioning System (RSP) as a backend system. To transfer the necessary network credentials and other personalization data, a secure channel is established. The secure channel protocol ensures confidentially, integrity and authenticity of the transferred data [RSP.21].

Conceptually, the eSIM platform prevents any exchange of data between different security domains. This applies to every security domain and represents an important architectural security feature. Apart from the difference regarding the modifiable content of the hardware element (remote SIM provisioning), eSIMs with an activated MNO profile behave similar to removable SIM cards. The focus remains on the hardware security to protect sensitive content isolated from the mobile device.

SAM enabled eSIM

The existing eSIM architecture with its focus on MNO requirements is being expanded upon by the SAM security domain (SAM-SD). As shown in Figure 1, this domain is isolated from the MNO specific security domains (ISD-P). SAM is an important standardization item at GSMA [GSMA-SAM] and GlobalPlatform. Access to the SAM-SD will be granted to trusted third party service providers and application providers, depending on policies to be developed. Applications for intended use cases deploy a Java Card applet with security relevant contents in a dedicated Application Service Provider Security Domain (ASP-SD). The hardware element acquires thereby the character of a platform, with neither chip manufacturer nor OEM having exclusive authority over this domain.

The trusted relation between involved entities of the SAM ecosystem relies on a PKI, the details of which are currently being specified. In the operational context, this concerns the Application Service Provider (ASP),

the SAM Subscription Manager (SAM-SM) and the SAM-SD on the eSIM itself, all pointing to the same root certificate in the same chain of trust. This offers a reliable isolation and has no interdependencies within different solutions. Therefore, the SAM-SD and the contained applets are not dependent on the activation status of an MNO-Profile and are operational on their own terms without the need of a telecommunications contract. For instance, users would be able to switch their MNO profile without disabling personalized eID, ticketing or payment applets secured by the same eSIM since those are not part of the ISD-P.

The fine-granular separation of use cases can be realised by several individual ASP-SDs existing within the general SAM-SD. Maintenance of the applications and their credentials is performed by the respective ASP, and in general handled independently of MNO and OEM through a dedicated backend system (see Figure 1). With release 17 of the ETSI UICC specification TS 102 221, it is possible to host multiple active profiles at once on an eSIM [TS-102-221]. These profiles are able to communicate via Logical SE Interfaces (LSI) to facilitate the separation without mutual restrictions. Thus, the SAM-SD does not conflict with one or multiple active MNO profiles and hence using the SAM-SD is possible without limiting mobile communications.

Conclusion

Several interest groups are expecting extensive market coverage of eSIM solutions rendering traditional SIM obsolete within the next few years [McK-eSIM]. In all likelihood, eSIMs will also be available for low-cost models. In addition to governmental organisations, private sector organisations can therefore also make use of the emerging SAM framework and secure their applications for the general user base. In particular, a mobile eID based on SAM can seamlessly replace other identification techniques, e.g. the broadly used video identification which is considered less secure. The possibilities for service providers to reliably secure their existing or emerging applications with this technology represent a significant improvement with respect to the solutions available today. To this end, the specific rules for participation in this ecosystem must be clarified with the various stakeholders in the time to come.

The benefits of the SAM Security Domain align with the goals of the BSI to increase cybersecurity for all parts of the society and in particular for citizens of the EU. Compared to already available alternatives, it is a promising technological development for use cases with a high security demand. In particular, the utilization within governmental tasks is recommended.

The BSI invites all stakeholders, including manufactures of secure elements, backend providers, MNOs and OEMs of mobile devices, and civil organizations to contact us by Mobile-eID@bsi.bund.de for further discussions.

Abbreviations

ASP	Application Service Provider
CC	Common Criteria
ECASD	Controlling Authority SD for the eUICC/eSIM
eID	electronic identity
eIDAS	electronic IDentification, Authentication and trust Services
eSIM	embedded SIM – personalized eUICC
EUDI	European Digital Identity
eUICC	embedded UICC – Platform for the eSIM and SAM in the future
IoT	Internet of Things
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root

LoA	Level of Assurance
LSI	Logical SE Interfaces
MNO	Mobile Network Operator
NAA	Network Access Application
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
RSP	Remote SIM Provisioning
SAM	Secured Applications for Mobile
SD	Security Domain
SIM	Subscriber Identity Module
SM	Subscription Management
SP	Service Provider
SSD	Suplementary Security Domain
TS	Technical Specification
UICC	Universal Integrated Circuit Card – Platform for SIM Cards

References

[eIDAS-Reg] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[Eusm-SAM] Eurosmart: "GSMA SAM solution: opportunities and challenges for mobile identity", 2021, https://www.eurosmart.com/european-mobile-identity-recommendations-on-sam-technology/, accessed 11 May 2023

[Eusm-Wallet] Eurosmart: "European Digital Identity Wallet: Why do we need level 'high' (eIDAS) & level 'high' (Cybersecurity Act)", 2023, https://www.eurosmart.com/european-digital-identity-wallet-why-do-we-need-level-high-eidas-level-high-cybersecurity-act/, accessed 11 May 2023

[GSMA-IoT] GSMA: "IoT SAFE: Robust IoT security at scale. The why, what and how of securing IoT applications and data.", 2021, https://www.gsma.com/iot/wp-content/uploads/2021/06/IoT-SAFE-Whitepaper-2021.pdf, accessed 11 May 2023

[GSMA-SAM] GSMA: "Secured Applications for Mobile – Requirements", Official Document SAM.01, Version 1.0, 2021

[McK-eSIM] McKinsey: "E-SIM for consumers – a game changer in mobile telecommunications?", 2016, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/e-sim-for-consumers-a-game-changer-in-mobile-telecommunications, accessed 11 May 2023

[SGP.21] GSMA: "SGP.21: RSP Architecture", Version 3.0

[TCA-SAM] Trusted Connectivity Alliance: "Realising the Potential of Secured Applications for Mobile (SAM): A TCA Position Paper", 2023, https://trustedconnectivityalliance.org/wp-content/uploads/2023/02/TCA_SAM_PositionPaper_FINAL.pdf, accessed 11 May 2023

[TS-102-221] ETSI, TS 102 221 V17, "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 17)"