EUROSMART
The Voice of the Digital Security Industry

20 July 2020

Leveraging the 5G SIM for enhanced subscriber privacy

Eurosmart welcomes the initiative of Trusted Connectivity Alliance (TCA) to leverage the capabilities of the 5G SIM / eSIM to enhance subscriber privacy. In previous network generations (2G, 3G, 4G), the identifier of the subscriber, aka IMSI, is transmitted in clear text over the air interface and hence is subject to certain threats. So called IMSI catchers can be obtained easily at relatively low cost and are used by attackers to get hold of the IMSI and consequently retrieve valuable and highly private information such as the location of the subscriber, the SMS sent or even data being transferred.

In 5G, this security weakness is addressed. The 5G successor of the IMSI, the Subscriber Permanent Identifier (SUPI), can be encrypted and transmitted over air as a Subscriber Concealed Identifier (SUCI). The key used to encrypt the SUPI is securely stored within the 5G SIM / eSIM. According to the 3GPP specifications, the encryption procedure as such can either be performed within the device or within the 5G SIM / eSIM.

TCA created a whitepaper stating that there are certain scenarios where SUPI encryption is not activated - either on the network side or within the device. Eurosmart supports the TCA position that protection of the subscriber privacy, i.e. the encryption of the SUPI, shall be made mandatory. Respective regulatory measures should be put in place to guarantee that this important feature is activated throughout the EU. Eurosmart further agrees with TCA that performing the SUPI encryption and thus the security relevant operation within the 5G SIM / eSIM has huge advantages. By mandating the encryption to be done within the 5G SIM / eSIM, the sensitive key used for the encryption does not need to be transferred to the mobile device and remains within a secure environment.

The Mobile Network Operator (MNO) is responsible for the security of the network and the protection of the subscriber. The MNO owns and controls the 5G SIM / eSIM configuration. If the SUCI calculation is done within the 5G SIM / eSIM, the MNO will own the security and privacy of the SUPI end-to-end, i.e. from the 5G SIM /eSIM to the network. On the contrary, devices are under the control of the device manufacturers, thus responsibility for subscriber privacy will be split between the MNO and the device manufacturer in case the SUCI calculation is done within the device.

Making sure that subscriber privacy is applied appropriately and interoperable across all different devices (e.g. different models from different manufacturers, devices for consumers or the IoT) within the network of the MNO is a challenge. Providing the SUCI calculation within the 5G SIM / eSIM will therefore reduce fragmentation and increase interoperability.

Furthermore, beyond supporting the privacy of users, the encryption of SUPI is also relevant to cybersecurity of critical infrastructures. 5G is instrumental for the advent of future technologies such

as IoT, connected car, or Industry 4.0. Weaknesses in the network architecture allowing to locate a connected device, or even intercept some of its communication could be exploited to threaten the security of critical infrastructures. For instance, it could become possible for an attacker to impersonate another device or to tamper with its rightful communication. In that respect, this issue shall also be considered in the light of cybersecurity and shall be taken into consideration when (1) assessing the security of 5G networks and (2) for the implementation of the NIS Directive within Member States.

Taking into consideration these threats, both to the privacy of user but also to the security and resilience of critical infrastructures and Operator of Essential Services (OES), Eurosmart calls for:

- the definition of an ad hoc security certification scheme covering SUPI encryption within 5G SIM / eSIM under the Cybersecurity Act (CSA), taking into consideration the constraints of the market;

- regulatory act mandating (1) SUPI to be encrypted within the 5G SIM / eSIM, and (2) 5G SIM / eSIM to be mandatorily security certified, to demonstrate its security capabilities.

In Summary

Eurosmart echoes TCA's position that (1) protection of the 5G subscriber permanent identifier (SUPI) shall be made mandatory and (2) performing the subscriber privacy related encryption (SUCI calculation) shall be done within the 5G SIM / eSIM. Eurosmart also higlights that these issues have direct consequences on the cybersecurity and resilience of critical infrastructures and Operator of Essential Services (OES), and as such shall also be considered in the light of cybersecurity legislation (NIS Directive).

In addition, Eurosmart believes that respective regulatory measures should be put in place to:

- define an ad hoc security certification scheme covering SUPI encryption within 5G SIM / eSIM under the Cybersecurity Act (CSA), taking into consideration the constraints of the market;

- require (1) SUPI to be encrypted within the 5G SIM / eSIM, and (2) 5G SIM / eSIM to be mandatorily security certified, to demonstrate its security capabilities.

Abbreviations

CSA	EU Cybersecurity Act (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act))
eSIM	embedded Subscriber Identity Module
IMSI	International Mobile Subscriber Identity
IoT	Internet Of Thing
MNO	Mobile Network Operator
NIS	Directive on Network and Information Security (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union)
OES	Operator Of Essential services
SIM	Subscriber Identity Module
SMS	Short Message Service
SUCI	Subscriber Concealed Identifier
SUPI	Subscriber permanent identifier
TCA	Trusted Connectivity Alliance

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international 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 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**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), 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 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

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com