EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SPECIFICATIONS FOR EUICC CERTIFICATION UNDER THE EUCC SCHEME

Version 1.0 for public consultation

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION AND CONTEXT

1.1 INTRODUCTION

This document is related to the certification of the embedded Universal Integrated Circuit Card (eUICC) under the EUCC scheme[1], and this version has been prepared for public consultation to take place from Q2 2024.

For the consultation process, the EU Survey tool will be used that enables parties to participate online and provide feedback. For that purpose, after having read this document, you may participate in the public consultation via the link provided on the ENISA website dedicated to certification: https://certification.enisa.europa.eu/index_en

The eUICC is a secure element that contains one or more subscription Profiles. Each Profile enables the eUICC to function in the same way as a removable SIM issued by the operator that created it. An eUICC is an embedded secure element that is integrated into devices, in contrast to the traditional UICC which is a removable card.

The eUICC is key to safeguarding the end customer's and the operator's security. It ensures secure access to networks and a subscriber's account, as well as related services and transactions. Therefore, it is essential to enhance consumer and industry confidence in eUICCs.

All eUICC types presented in this report are considered to be certified using the European Cybersecurity Scheme on Common Criteria (EUCC).

The EUCC scheme covers the common criteria certification of smart cards. Accordingly, the certification of the eUICC smartcard component can be addressed by the EUCC, provided some optimisation of evaluation procedures to match requirements of the mobile market can be implemented. The certification of the eUICC will not require a new certification scheme.

Efforts shall also be made so that the specifications of the eUICC implement functional, security and certification requirements identified and match, where possible, other relevant regulations, such the European Digital Identity (EUDI) Regulation[2] and the Cyber Resilience Act (CRA)[3].

Regarding the EUDI Wallet, this document considers the possibility to use the eUICC as a support to hosting EUDI Wallet applets, but acknowledges the possibility that the EUDI Wallet can support other implementations[4], currently outside of the scope of this scheme. The EUDI Regulation remains technologically neutral and does not favor one architecture over the other, hence the eUICC certification can be also useful to support one or more EUDI Wallet components but it is only one option out of the different possibilities to certify the Wallets.

[1] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), OJ L, 2024/482, 7.2.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482, accessed May 2024.
[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183, accessed May 2024.
[3] Provisionally agreed text between EU co-legislators adopted by the European Parliament on 12.03.2024: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html, accessed May 2024.
[4] https://www.gsma.com/gsmaeurope/resources/architecture-considerations-for-eidas-2-0/, accessed May 2024.

Regarding the CRA, it is noted that manufacturers of eUICC fall under the scope of the future CRA and that 'smart cards or similar devices' are considered 'critical products with digital elements' under the CRA. Once the CRA will become applicable, this product category will be subject to mandatory third-party assessment and could potentially be subject to mandatory European cybersecurity certification of at least level substantial. Furthermore, the European cybersecurity certification can be used to demonstrate presumption of conformity with the requirements of the CRA. The document will be further aligned with the specific requirements of the CRA in a next iteration.

This document exclusively covers eUICCs for consumer devices and IoT eUICCs, as defined by the GSMA specifications. While it does not specifically address eUICCs for Machine-to-Machine (M2M), the optimisations presented herein can be beneficial to M2M contexts as well.

In this document, the terms "eUICC for consumer devices" and "IoT eUICCs" are used interchangeably. Specific terminology is employed only when necessary to clarify particular contexts or distinctions.

1.2 CONTEXT

These specifications are part of the ENISA work under the EU5G AHWG, considering ENISA has been requested in 2021 by the European Commission to prepare a candidate European cybersecurity certification scheme for 5G networks that would take into account:

- the GSMA's Network Equipment Security Assurance Scheme[5], and
- relevant Common Criteria Protection Profiles (or Technical Domains) for embedded Universal Integrated Circuit Card (eUICC), in conjunction with relevant specifications for the evaluation process with reference to GSMA's scheme for secure provisioning and use of subscriber identity (GSMA SAS-up, SAS-SM)[6].

They take benefit of the EUCC scheme adopted under Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[5] https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed May 2024.
[6] https://www.gsma.com/security/security-accreditation-scheme/, accessed May 2024.

2. REFERENCES, DEFINITION OF TERMS, ABBREVIATIONS

2.1 REFERENCES

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, CSA)[7]

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council[8]

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93[9]

Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)[10]

Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework[11]

Common Criteria for Information Technology Security Evaluation (CC), Version 2022, ISO/IEC 15408, available at https://www.commoncriteriaportal.org/cc/index.cfm

Common Methodology for Information Technology Security Evaluation (CEM), Version 2022 ISO/IEC 18045, available at https://www.commoncriteriaportal.org/cc/index.cfm

[7] 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), OJ L 151, 7.6.2019, p. 15, https://eur-lex.europa.eu/eli/reg/2019/881/oj, accessed May 2024.
[8] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, OJ L 316, 14.11.2012, p. 12, https://eur-lex.europa.eu/eli/reg/2012/1025/oj, accessed May 2024.
[9] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 13.8.2008, p. 30, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008R0765, accessed May 2024.
[10] See footnote 1.
[11] See footnote 2.

2.2 DEFINITION OF TERMS

This document uses the definitions of terms given in the EUCC scheme. In addition, the following terms are relevant for this document:

Applet	Application hosted by the eUICC.
App	Application installed in the user's mobile device (e.g., Android or iOS Apps).
Assurance	Grounds for confidence that an ICT product, ICT service or ICT process as target of evaluation meets the security functional requirements (cf. ISO/IEC 15408-1, definition of terms).
Assurance level	Basis for confidence that an ICT product, ICT service or ICT process meets the security requirements of a specific European cybersecurity certification scheme, indicates the level at which an ICT product, ICT service or ICT process has been evaluated but as such does not measure the security of the ICT product, ICT service or ICT process concerned (cf. CSA, article 2.22).
Attack potential	Measure of the effort to be expended in attacking an ICT product, ICT service or ICT process as target of evaluation, expressed in terms of an attacker's expertise, resources and motivation (cf. ISO/IEC 15408-1, definition of terms).
UICC	A Secure Element as defined by ETSI TC SET specifications.
eUICC	A UICC with remote provisioning capability.
EUDIW	A European Digital Identity Wallet as defined in Regulation (EU) 2024/1183 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a the framework for a European Digital Identity Framework .
SAM	GSMA approach named Secured Applications for Mobile[12]. Allows the division of the eUICC into several "domains" where service providers could host their secure applets independently and outside of any eUICC telco profile.
CSP	Cryptographic Service Provider[13] providing a trusted and certified cryptography toolbox to applet developers that reduces the overall effort and time demand for applet development and certification.
JCP	Java Card™ enables secure elements, such as smart cards and other tamper-resistant security chips, to host applications, called applets, which employ Java technology. The Java Card Platform (JCP) specification provides the basis for cross-platform and cross-vendor applet interoperability.

[12] Latest version is accessible here : https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/11/SAM.01-v1.1-1.pdf, accessed May 2024.
[13] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03181/TR-03181_node.html, accessed May 2024.

ADV_FSP (Functional specification)

This common criteria assurance family contains requirements upon the description of the TSF interfaces (TSFI). The TSFI consist of all means for users to invoke a service from the TSF (by supplying data that is processed by the TSF) and the corresponding responses to those service invocations. If an action available through an interface can be traced to any of the SFRs contained in the ST, then that interface is SFR-enforcing. Interfaces to actions that SFR-enforcing functionality depends on, but need only to function correctly in order for the security policies of the TOE to be preserved, are termed SFR- supporting. Interfaces to actions on which SFR-enforcing functionality has no dependence are termed SFR-non-interfering. For an interface to be SFR-supporting or SFR non-interfering it must have no SFR-enforcing actions or results. In contrast, an SFR-enforcing interface may have also SFR-supporting actions.

AGD_OPE (Operational user guidance)

Requirements for operational user guidance help ensure that all types of users are able to operate the TOE in a secure manner. It should be excluded that the TOE can be used in a manner that is insecure but that the user of the TOE would reasonably believe to be secure. Operational user guidance is the primary vehicle available to the developer for providing the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions.

AGD_PRE (Preparative procedures)

Preparation requires that the delivered copy of the TOE is accepted, configured and activated by the user to exhibit the protection properties as needed during operation of the TOE. The preparative procedures provide confidence that the user will be aware of the TOE configuration parameters and how they can affect the TSF.

ATE_FUN (Functional tests)

Functional testing performed by the developer provides assurance that the tests in the test documentation are performed and documented correctly. The correspondence of these tests to the design descriptions of the TSF is achieved through the Coverage (ATE_COV) and Depth (ATE_DPT) families.

ATE_COV (Coverage) This family establishes that the TSF has been tested against its functional specification (ADV_FSP). This is achieved through an examination of developer evidence of correspondence.

ATE_DPT (Depth) The components in this family deal with the level of detail to which the TSF is tested by the developer. Testing of the TSF is based upon increasing depth of information derived from additional design representations and descriptions. The objective is to counter the risk of missing an error in the development of the TOE. Testing that exercises specific internal interfaces can provide assurance not only that the TSF exhibits the desired external security behaviour, but

also that this behaviour stems from correctly operating internal functionality.

ATE_IND (Independent testing)

The objectives of this family are built upon the assurances achieved in the ATE_FUN, ATE_COV, and ATE_DPT families by verifying the developer testing and performing additional tests by the evaluator.

ALC_FLR (Flaw remediation)

Flaw remediation ensures that flaws discovered by the TOE consumers will be tracked and corrected while the TOE is supported by the developer. While future compliance with the flaw remediation requirements cannot be determined when a TOE is evaluated, it is possible to evaluate the procedures and policies that a developer has in place to track and repair flaws, and to distribute the repairs to consumers.

ADV_TDS (TOE design) The requirements of the TOE design family are intended to provide information so that a determination can be made that the security functional requirements are realised. The goal of design documentation is to provide sufficient information to determine the TSF boundary, and to describe how the TSF implements the Security Functional Requirements. As assurance needs increase, the level of detail provided in the description also increases. The amount and structure of the design documentation will depend on the complexity of the TOE and the number of SFRs. The assurance provided for very complex TOEs will benefit from the production of differing levels of decomposition in describing the design, while very simple TOEs do not require both high-level and low-level descriptions of its implementation.

Third Party Applets — Applets provided by a Service Provider different from the Telecom Operator. These applets are loaded into the eUICC in SAM Security Domains and not inside Telecom Profiles.

2.3 ABBREVIATIONS

API	Application Programming Interface
AHWG	Ad Hoc Working Group
ATE	Automatic test equipment or automated test equipment
CEM	Common Evaluation Methodology
CC	Common Criteria
CSP	Cryptographic Service Provider
ECASD	eUICC Controlling Authority Security Domain
ETSI	European Telecommunications Standards Institute
ETSI TS	ETSI Technical Specification
eSIM	See eUICC, “eUICC”, “eSIM” , “iSIM” and “ieUICC” are used interchangeably in this report

eUICC	Embedded Universal Integrated Circuit Card
EUDIW	European Digital Identity Wallet
GP	GlobalPlatform
GSMA	GSM Association
ICCID	Integrated Circuit Card Identification
IC	Integrated Circuit
ICT	Information and Communications Technology
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
IMSI	International Mobile Subscriber Identifier
JCP	Java Card Platform
MNO	Mobile Network Operator
OEM	Original Equipment Manufacturer
RSP	Remote SIM Provisioning
SAM	(GSMA) Secured Applications for Mobile
SE	Secure Element
SD	Security Domain
SFR	Security Functional Requirements
SoC	System on Chip
ST	Security Target
TOE	Target of evaluation
TSF	TOE Security Functions
TSFI	TSF Interfaces

3. EUICC: DEFINITION AND TYPES

3.1 eUICC DEFINITION

The terms eSIM and eUICC in this document are used interchangeably. The following paragraphs, collected from the GSMA eSIM whitepaper, March 2018[14], with some simplifying adaptations within brackets, present what the eSIM essentially is and what it does. For more details and consumer and business benefits of the system, please consult the GSMA eSIM whitepaper.

"The ubiquitous SIM card […] provides a secure means for authenticating devices onto networks, all inside a removable "Secure Element", which is easily transferrable between mobile devices. Although the role of the SIM itself is not changing, the GSMA has defined a radical new way to load it into devices. Now the SIM may be securely downloaded into a 'Secure Element' that can be permanently embedded inside any type of device.

[…] The change from the Removable SIM to an eSIM provides benefits for many players:

- **For everyone,** eSIM provides an equivalent level of security as the removable SIM card. This is vital as it is the subscription credentials stored on the SIM card that enable secure and private access to mobile networks. It also supports the integrity of the billing process, especially in roaming scenarios.
- **For the device end user,** eSIM enables simplified management of subscriptions and connections. End users will no longer have to manage several SIM cards.
- **For organisations,** eSIM enables remote management of subscriptions. This is a significant benefit where devices are not managed by the end user or are not be readily accessible (for example due to operational scale, making individual device management cost prohibitive). This enables pioneering categories of connected devices.
- **For distributors,** simplified logistics are possible, customisation for specific operators or regions may be reduced.
- **Operators** will have simpler means to expand their businesses into emerging markets, for example, automotive, wearables and consumer electronics. SIM card distribution costs will be eliminated, and eSIMs will enable new distribution models for devices and for marketing of subscriptions.
- **Device Manufacturers,** can exploit the reduced space within their products to make smaller devices. Their products could also be made more tolerant to environmental factors such as dampness, temperature and vibration as they can be hermetically (completely airtight) sealed. Manufacturers can also leverage eSIMs to optimise supply chain processes.

[…] The integrity of traditional SIM cards is safeguarded by using secure facilities for their manufacture, which includes loading of software and operator credentials. Operator logistics channels then distribute the SIM cards to the required endpoints, for example retail shops, retail partners or enterprise customers managing fleets of connected devices. eSIM extends the

[14] https://www.gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf, accessed May 2024.

reach of the secure facilities from specific physical locations, to any location where the device can be reached over the internet. eSIM protocols provide security and integrity for data transfer.

[…] With Remote SIM Provisioning, there are no traditional SIM cards[15]. Instead there is an embedded SIM (called an eUICC), which may be soldered inside the mobile device, that can accommodate multiple SIM Profiles – each Profile comprising of the operator and subscriber data that would have otherwise been stored on a traditional SIM card.

[…] [The] end user sets up a contract with their chosen mobile network operator, and in the case of a Consumer solution, instead of receiving a SIM card they will receive instructions on how to connect their device to the operator's Remote SIM Provisioning system.

Should the end user wish to [add or] change operator, they can set up a contract with the new operator […] and download the new Profile. The end user is now able to switch between the two Profiles, to connect their device to whichever operator's network the end user selects […].

[…] A Profile comprises the operator data related to a subscription, including the operator's credentials and potentially operator or third-party SIM based applications. The **secure element** in the eSIM solution is called the **eUICC**, this can accommodate multiple Profiles. Profiles are remotely downloaded over-the-air into a eUICC. Although the eUICC is an integral part of the device, the Profile remains the property of the operator as it contains items "owned" by the operator (IMSI, ICCID, security algorithms, etc.) and is supplied under licence. The content and structure for interoperable Profiles stored on eUICCs are similar to those installed on traditional SIMs. [Operator Profiles are stored inside Security Domains within the eUICC and are implemented using GlobalPlatform standards. These ensure that it is impossible for any Profile to access the applications or data of any other Profile stored on the eUICC. The same mechanism is currently in use within SIM cards to ensure payment applications are kept secure[16].

3.2 eUICC TYPES

3.2.1 Type 1 - eUICCs for consumer and IoT devices not requiring third party applets

eUICCs of this type are designed for consumer and IoT devices that do not require third-party applets, being used exclusively for telecommunications.

The following figure illustrates the different eUICC components.

[15] Although written assuming the eUICC is a permanent fitting in the device (e.g. soldered) it is possible for eSIM deployments to make use of removable SIM formats.
[16] SGP.22 "GSMA RSP Technical Specification"

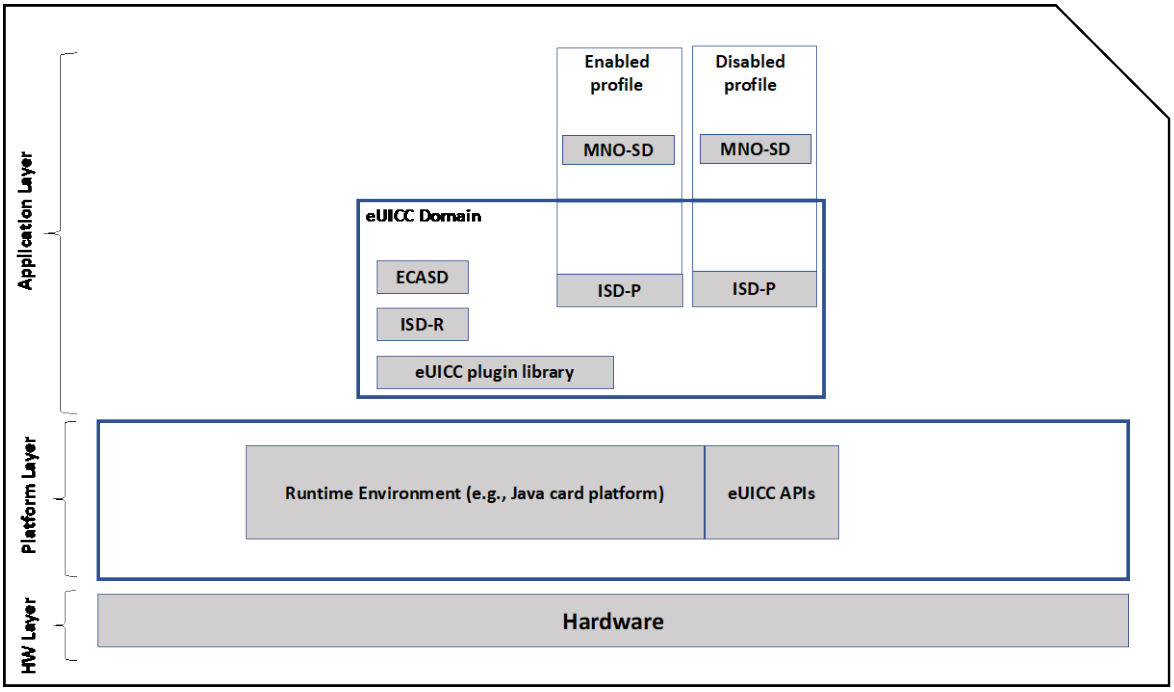

Figure 1: eUICC basic components

The architecture is composed of the:

Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality.

The ISD-P is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is also used for updating the Profile Metadata on behalf of the MNO.

The ISD-R is responsible for the creation of new ISD-Ps and life-cycle management of all ISD-Ps. An ISD-R shall be created within an eUICC at the time of manufacture.

The MNO-SD is the on-card representative of the MNO Platform. It contains the MNO Over-The-Air (OTA) keys and provides a secure OTA channel.

The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for the secure storage of credentials used to enforce trust in the identities of Actors (eUICC, remote Actors such as SM-DS or SM-DP+) and provides security functions used during key establishment and eUICC authentication.

Platform Layer: a set of functions providing support to the Application Layer:

- A Telecom Framework providing network authentication algorithms;
- A Profile Package Interpreter translating Profile Package data into an installed Profile;
- Profile Rules Enforcer which comprises the Profile Policy Enabler (Profile Policy verification and enforcement functions) and the enforcement of Enterprise Rules.
- The Runtime Environment (for example Java card platform).

Hardware Layer: a secure IC composed of a processing unit, memories, security components and Input/Output (I/O) interfaces. The eUICC hardware is a tamper resistant element that is either an eUICC chip or integrated into a system-on-chip (SoC).

Note: According to ETSI TS 102 221, the eUICC may support Logical Secure Element interfaces, which allows it to host multiple logical secure elements, and thus enables the support of multiple enabled telco profiles on one eUICC.

3.2.2 eUICCs for consumer devices hosting third party applets

These eUICC types offer the ability to host secured services and sensitive data including mobile ID and other trust services. Such hosting shall be interoperable and accessible to all service providers from their backend(s) via standardized interfaces and without significant dependency on specific actors. Sensitive user-based information would be securely stored in the eUICC of the mobile and in an isolated way ensuring data protection & privacy.

The hereabove requirement is met by the GSMA approach named Secured Applications for Mobile - SAM.

The SAM approach allows the division of eUICC into several “domains” where service providers could host their secure applets as illustrated in the following figure. Applets will operate independently and outside of any telco profile as illustrated by the following figure.

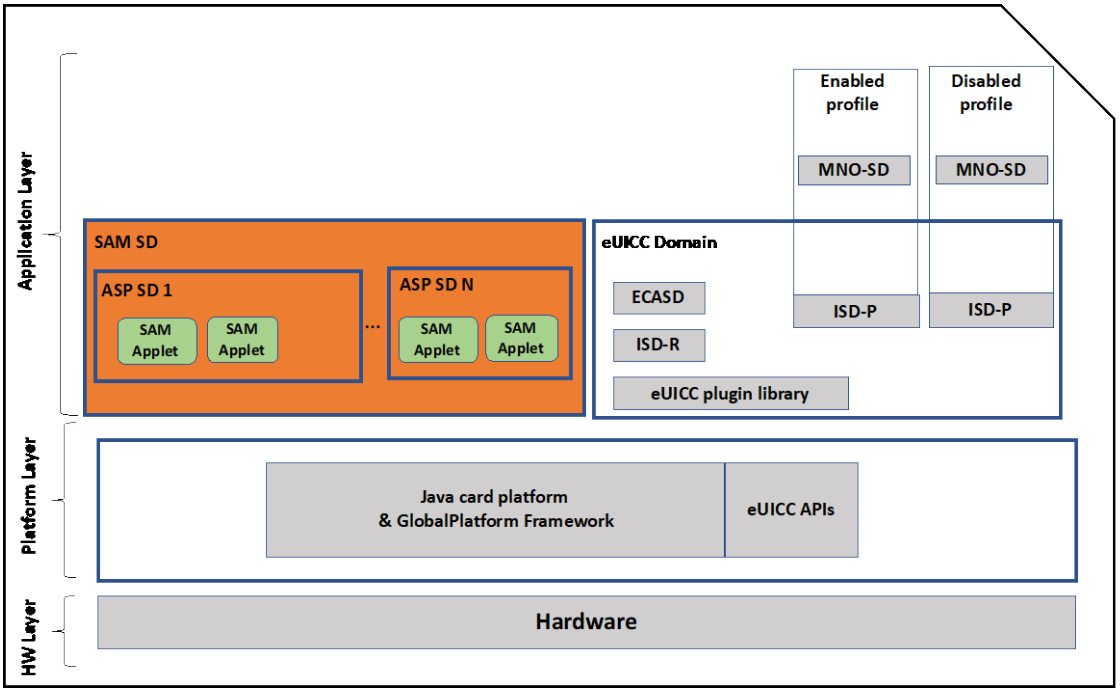

Figure 2: eUICC augmentation as specified by the SAM concept

Note: According to ETSI TS 102 221, the eUICC may support Logical Secure Element interfaces, which allows it to host multiple logical secure elements, and thus enables the support of multiple SAM SDs.

SAM supports secure spaces for applets, so-called SAM security domains, which are separated from those used by the mobile sector. All SAM security domains are isolated from each other and can be allocated to dedicated ecosystems like the EUDIW ecosystem. The SAM security domains are installed during production of the eUICC by the eUICC supplier and, after that, managed by another entity, the SAM Service Manager, throughout their life-cycle.

The specifications of the SAM concept allow the owner of a SAM security domain to select the entity that manages the domain. Only this entity, the SAM Service Manager, which, on behalf of the Application Service Provider, is in charge of managing SAM Applets through SAM

Commands using the ASP certificate. SAM SM interacts with a SAM-SD for which it has access to ASP credentials..

The responsible SAM Service Manager can generate individual secure spaces, so-called sub-domains, within a SAM security domain. These are securely isolated from each other and can be allocated to specific application providers to host their applets. After generating a sub-domain, the SAM Service Manager hands over the access rights to the application providers. From that point onwards, only these can access and manage the contents of the sub-domain (e.g. personalization of the applet).

There are two types of eUICC supporting SAM, depending on whether the third-party applets require EUCC certification or not.

Type 2 - eUICC hosting applets subject to EUCC certification

Type 2 is designated for eUICCs that host third-party applets that are subject to EUCC certification, requiring a high security assurance level and operating in a separate security domain distinct from telco profiles, such as EUDIW applets.

In addition to the above, these eUICCs should support a Cryptographic Service Provider (CSP) to allow the certification of the applets independently from the underlying platforms: this optimisation would allow third-party applets on the eUICC that require EUCC certification to be certified just once, and this certification should be valid across all certified eUICC types, and would compensate the current composite CC (Common Criteria) approach that does not allow for an interoperable certificate for a third-party applet to be be scaled across all different certified eUICCs without going back to additional evaluation and recertification.

This cryptographic abstraction layer should be used to omit the need for physical testing on all platforms for applets, while still meeting high security level in the context of a complete solution (e.g., EUDIW). This is particularly relevant for post-issued applets that are loaded onto the platform after delivery to the end user and are intended to run on a wide range of different platform configurations, whereas the classical composite evaluation approach would require countless re-evaluations of the applet for each platform.The hereabove requirement could be met by the CSP approach.

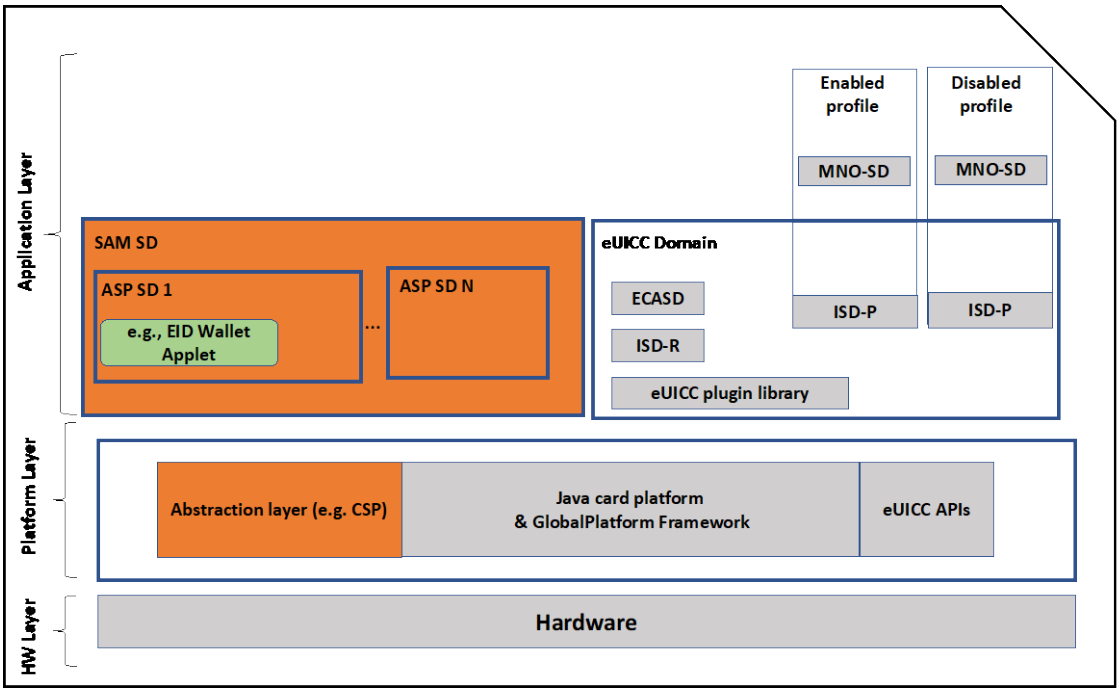

Figure 3: eUICC hosting applets subject to EUCC certification

Note: The CSP aims at providing a trusted and certified cryptography toolbox to applet developers that reduces the overall effort and time demand for applet development and certification. In current frameworks, an applet with high security demand requires a composite certification of the software (the applet) and the underlying platform (hardware and operating system). This is due to the fact that platforms provide basic cryptographic building blocks but not complex protocols that are used in demanding applets, such as e.g., EUDIW applets. Moreover, each eUICC platform may have guidance restrictions that have to be adhered to in order to securely implement such protocols. A composite certification of one or several applets for platforms of different vendors therefore results in a complexity that is not practical.

CSP is offering an abstraction layer to tackle this issue. It is not just a cryptographic library but it provides an API offering complex cryptography protocols and key management. Key material required by an applet is fully handled inside the CSP. In practice, security related tasks are triggered by the applet, but concrete cryptographic operations are executed in an isolated environment inside the CSP where sensitive assets are not transferred in an unencrypted manner to the applet or other unsecure environments. The CSP is intended to be installed on a secure element or a HSM which serves as platform for applications. In the case of the eUICC, the certified CSP is typically an extention of the eUICC's platform (e.g., Java Card Platform).

The CSP introduces significant benefits for application providers targeting higher certification levels for their applets:

1. The use of CSP's cryptography protocols and key management functions reduces the development and test effort for the applet significantly.
2. The evaluation and certification effort and time demand for the applet can be massively reduced, comparable to the effort for EAL2 (AVA_VAN.2), if all security-sensitive functions of the applet are covered by the CSP. Nevertheless, the combined security of the applet and CSP still achieve an overall security level comparable to EAL4 augmented with ALC_DVS.2 and AVA_VAN.5, since the business logic of the applet is independent from the sensitive operations that are protected by the high-assurance CSP.
3. The use of CSP's cryptography protocols and key management functions does also solve the issues related to the large number of eUICC types that would have to be targeted as platform for an applet. Since, provided that the sensitive functions are covered by CSP, the evaluation level for the applet can be reduced to a level lower than EAL4 (+AVA_VAN.5), such as EAL2 (AVA_VAN.2), and an evaluation and certification of the applet for each and every individual eUICC type is no longer necessary. The applet just needs to be certified once and operates with all certified eUICC types and CSP implementations.

Note: GlobalPlatform is actively working on standardizing the Cryptographic Service Provider (CSP). A work item has been initiated for this purpose. The details of the relevant document are as follows:

- Reference: GPC_SPE_230
- Name: GlobalPlatform Card Specification - Amendment N Cryptographic Service Provider.

Type 3 - eUICC with applets not subject to EUCC certification

Type 3 is designated for eUICCs that host third-party applets which are not subject to EUCC certification but require a high security assurance level, operating in a separate security domain distinct from telco profiles, such as payment applets subject to EMVCO certification[17].

[17] https://www.emvco.com/processes/common-payment-application-cpa-approval-process/

There is no regulation providing for EUCC certification on payment applets. For this type, only the SAM is required; the CSP is not required because the composite evaluation does not apply. Nevertheless, the use of CSP may be convenient in this case as well: applets may rely on CSP cryptographic services instead of implementing their own.

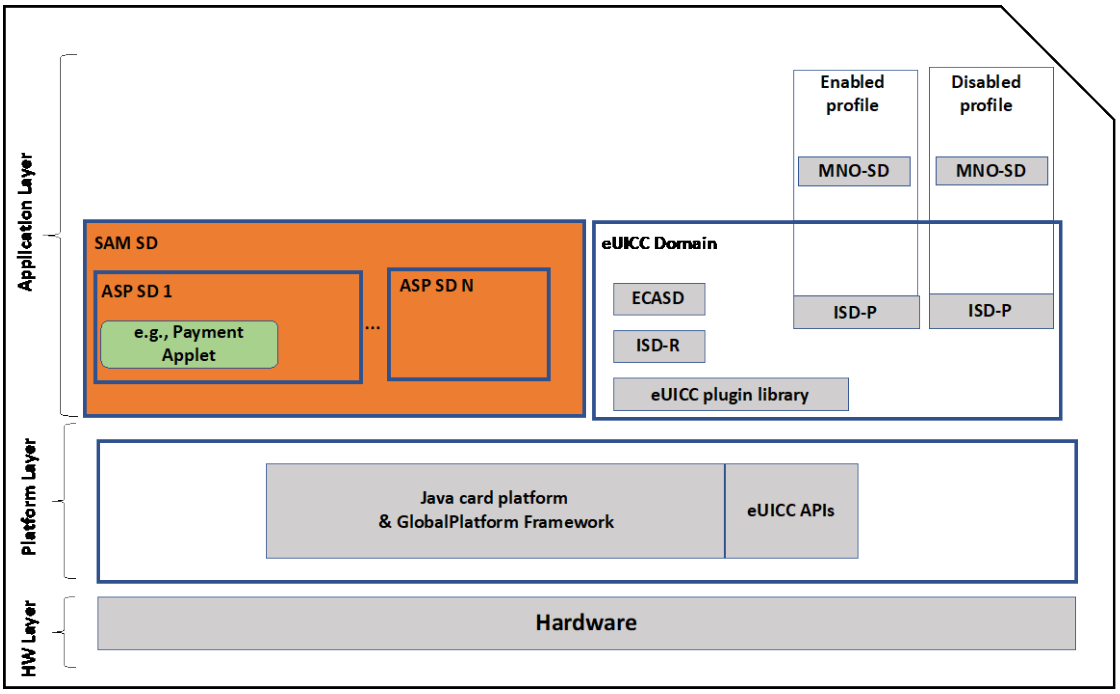

Figure 4: eUICC for third party applets not subject to EUCC certification

3.2.3 Type 4 - eUICC with CSP-Enabled support for applets within telco profiles

Type 4 is designated for eUICCs that host MNO's applets - that are not considered as third-party applets - within telco profiles and require CSP crypto services. eUICCs of this type do not require a SAM.

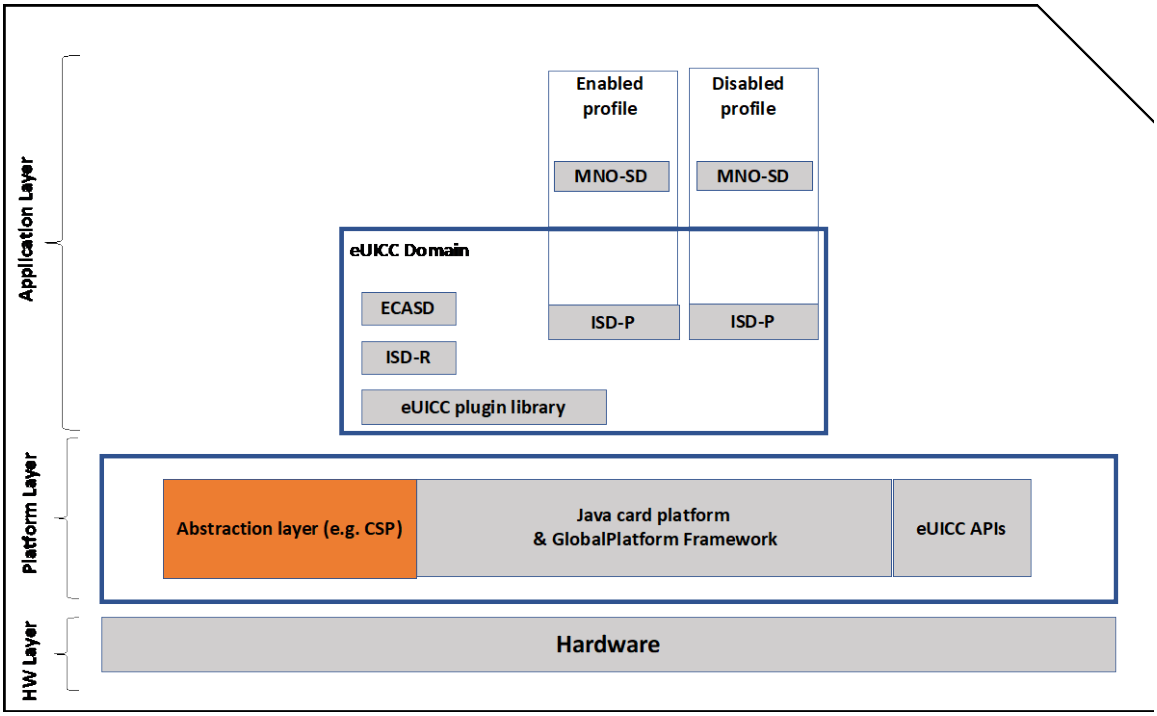

Figure 5: eUICCs for consumer and IoT devices requiring CSP services

3.2.4 Mapping between eUICC types and components

The following table provides the mapping between eUICC types and components. It shows, for each type, the required eUICC components.

eUICC components	Type 1	Type 2	Type 3	Type 4
eUICC hardware	x	x	x	x
eUICC Runtime Environment (e.g. Java Card Platform JCP & Global Platform framework)	JCP strongly recommended	JCP & GP framework	JCP & GP framework	JCP & GP framework
eUICC RSP	x	x	x	x
SAM		x	x	
CSP		x		x
Patch mechanism	x	x	x	x
Applets subject to EUCC certification		x		x
Applets not subject to EUCC certification	x		x	x

Table 1: Mapping between eUICC types and components

3.2.5 Mapping between eUICC types and use cases

The table below categorizes each eUICC type based on its specific use cases. Types 1 and 4 are applicable to both consumer and IoT devices, while types 2 and 3 are exclusively for eUICCs in consumer devices.

eUICC types	eUICC for consumer devices	IoT eUICCs

Type 1	x	x
Type 2	x	
Type 3	x	
Type 4	x	x

Table 2: eUICC types and their Use Cases in consumer and IoT Devices

4. CERTIFICATION OF EUICC

4.1 GENERAL STATEMENT

Certification according to CSA schemes is voluntary. Where an eUICC is to be certified, the following requirements **SHALL** apply, unless **SHOULD** is used to refer to a recommendation.

4.2 CERTIFICATION SCHEME

The eUICC components **SHALL** be certified under the EUCC scheme at EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

ALC_FLR.2 **SHOULD** be covered to support the vulnerability management and disclosure requirements as defined in the EUCC scheme.

eUICC components belongs to the technical domain “Smartcards and Similar Devices” as defined in the EUCC Implementing Act[18]. Thus, the eUICC components:

- **SHALL** be evaluated in accordance with the applicable state-of-the-art documents of the technical domain “Smartcards and Similar Devices” as defined in the EUCC scheme, Annex I.
- **SHALL** consider compliance with the relevant recommended certified protection profiles listed in EUCC scheme, Annex III.

Note: Protection Profiles for eUICC components are listed in Annex of this document. The possibility to incorporate them into Annex III of the EUCC scheme should be analysed once these PPs have been re-certified against the EUCC scheme.

The eUICC certificate **SHALL** indicate the eUICC type as requested in Annex VII b.2 of the EUCC and indicate the components from Table 1 that are part of the eUICC design.

4.3 CERTIFICATION REQUIREMENTS ON COMPONENTS

4.3.1 eUICC hardware

The eUICC hardware **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

4.3.2 eUICC java card platform (JCP)

Where the eUICC relies on a JCP, this platform **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 in composition with a previously certified underlying eUICC hardware.

Note: This requirement is optional for eUICC type 1 as defined in SGP.25, as type 1 is exclusively used for telecommunications or IoT, where there is no need for CSP, SAM, or third-party applets (see table 2).

4.3.3 eUICC java card platform (JCP) with GP framework

[18] https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-adoption-european-common-criteria-based-cybersecurity-certification-scheme

Where the eUICC relies on a JCP with GP framework, this platform **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 in composition with a previously certified underlying eUICC hardware.

4.3.4 eUICC RSP

The eUICC RSP **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 in composition with a previously certified underlying eUICC hardware.

4.3.5 Secure application on mobile (SAM)

The eUICC serving as secure platform hosting third-party applets (types 2 and 3) **SHALL** support new security domains for enabling access to those applets independently of telco profiles.

The new security domains **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 via the implementation of the SAM as specified by GlobalPlatform (GP) in the scope of the eUICC certificate.

4.3.6 Cryptographic abstraction layer (e.g.: CSP)

The eUICC, serving as a secure platform for hosting post-issued applets that are subject to EUCC certification (Types 2 and 4), **SHALL** support a harmonized cryptographic abstraction layer that encapsulates cryptographic operations and protocols, providing secure cryptographic services to applets through well-defined and standardized external interfaces (e.g., Cryptographic Service Provider (CSP)). The aim of this abstraction layer is to enable a certification of applets independently from the underlying platform, e.g., at a EAL2 (AVA_VAN.2) level, while maintaining a high security level at EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 of the combination platform and applet.

The abstraction layer that enables an independent applet certification **SHALL** be internationally specified and standardized to avoid fragmentation (e.g., by transferring BSI CSP to GlobalPlatform specifications). Only this standardized abstraction layer **SHALL** be used.

The abstraction layer that enables an independent applet certification **SHALL** be certified according to EUCC at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

Note: These requirements apply only to Types 2 and 4.

4.3.7 Vulnerability handling

All PPs/STs supporting the components eUICC **SHOULD** be augmented by ALC_FLR.2 to support the vulnerability management and disclosure requirements as defined in the EUCC scheme

4.4 PATCH MECHANISM

The eUICC **SHALL** support a patch mechanism for the OTA (over the air) secure updating of the eUICC software in the field. This mechanism **SHALL** verify the authenticity and integrity of received patches before their installation.

The patch mechanism **SHALL** be in the scope of the eUICC certificate as detailed in the EUCC scheme Annex IV.4 and therefore be certified at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

4.5 OPTIMISATION

The eUICC evaluations under EUCC **SHALL** have the following characteristics:

- Evaluation and certification SHALL fit industry standard timelines, providing best possible predictable and timely evaluation and certification.
- Evaluation SHOULD leverage industry-standard specifications (e.g.: GSMA eUICC specifications and test plans) and consider them as part of the evaluation evidence. This approach will reduce the effort developers must expend to prepare this evidence.

For these reasons, eUICC evaluation and certification under EUCC **SHOULD** consider the optimisations as defined in Annex A of this document.

ANNEX A – OPTIMISATION

The eUICC evaluation under the EUCC scheme should consider following optimisations to align with the requirements of the mobile market, that are not considered to necessitate the adaptation of the EUCC scheme itself.

A.1 OPTIMISATION OF eUICC CERTIFICATION

To ensure that the specifications of the eUICC fulfill the functional, security, and certification requirements identified and where possible, align with other regulations, such as the European Digital Identity (EUDI) Regulation[19], the necessary technical requirements and the correlating specifications (see Annex A.3.1) and protection profiles (see Annex B), for the different eUICC use-cases to be covered, have been identified.

For the eUICC, only these specifications and protection profiles should be used, to avoid fragmentation, and to allow easier updates of associated requirements.

A.2 OPTIMISATION OF THIRD-PARTY APPLETS CERTIFICATION

As described under 3.2.2.1 in the case of eUICCs Type 2, the use of a certified CSP will significantly redure the effort on the certification of third party applets, both in terms of assurance level required for these applets, and in terms of number of certificates needed for the different platforms.

A.3 OPTIMISATION OF EVALUATION PROCEDURES OF THE EUCC CERTIFICATION TO MATCH REQUIREMENTS OF THE MOBILE MARKET

A.3.1 Harmonisation between EUCC and eSA

The application of the EUCC for eUICC certification could be optimised to align with the GSMA eSA scheme in terms of effort and time-to-market. To make this feasible, the following steps should be followed:

1. The developer initiates two certification processes: one with the GSMA and another with an NCCA.

2. The evaluation of the eUICC is conducted under the eSA scheme by an ITSEF authorized by both the NCCA and GSMA.

3. The same ITSEF performs the EUCC evaluation according to the EUCC Implementing Act[20], by reusing the eSA evaluation results, mainly for the security target, vulnerability analysis, results of penetration testing, ATE, and AGD.

4. Both the GSMA and NCCA review the Evaluation Technical Report (ETR) issued by the ITSEF.

5. The GSMA issues an eSA certificate, and the NCCA issues an EUCC certificate.

[19] See footnote 2.
[20] See footnote 1.

This approach will expedite the certification process under EUCC and allow for the simultaneous acquisition of both eSA and EUCC certificates for the eUICC.

A.3.2 Consideration of GSMA specifications as part of certification evidences

For the purposes of evaluating the compliance of RSP eUICC with the EUCC, the following standards shall apply:

(a) the Common Criteria (CC);

(b) the Common Evaluation Methodology (CEM);

(c) The GSMA eUICC specifications listed in the table below.

The **eUICC evaluations** shall have the following **characteristics**:

- Evaluation and certification should fit industry standard timelines, providing best possible predictable and timely evaluation and certification.
- Evaluation and certification should accept industry standard specifications as sufficient.

For these reasons, eUICC evaluation and certification under EUCC should include the following **optimisations**:

- Evaluating and Certifying Bodies should consider the SGP.23-1 and SGP.26 functional testing done as required by GSMA schemes and checked by evaluators assigned by GSMA, provided the GSMA accredited evaluators have been also accredited by an EU Member State National Accreditation Body in accordance with the EU Accreditation Regulation and the provisions of the EUCC scheme, reusable and sufficient for ATE_FUN and ATE_COV, i.e. that all relevant standard functionality is already sufficiently tested. Functionality beyond the standard would be subject to normal ATE evaluation by the ITSEF.
- When Evaluating and Certifying Bodies assess eUICCs, those designed in accordance with the architectural standards of GSMA SGP.21 and technical guidelines of GSMA SGP.22 should be recognised as meeting the ADV_FSP.4 requirements (spanning work units ADV_FSP.4-1 to ADV_FSP.4-9) as outlined in the CC CEM. However, features surpassing these standards will need a standard ADV_FSP.4 assessment.
- eUICCs crafted in line with the technical guidelines of GSMA SGP.22, which outlines the expected remote provisioning functionality, would be deemed to meet AGD criteria. Again, any features that go beyond these standards would require a standard AGD evaluation.

The following table lists the GSMA eUICC specifications that could be used as part of the CC evidence for RSP eUICC evaluation. It maps each specification to the corresponding CC class. Some CC requirements are specific to a developer implementation (e.g., TOE proprietary design, security architecture, the mapping to SFRs, etc.), thus those requirements are beyond the standard and have to be provided by the developer to the evaluator addition to the GSMA eUICC RSP specifications.

eUICC spec number	eUICC spec title	ASE	ADV_FSP	ADV_TDS	ATE	AGD
Common specifications for eUICCs for consumer devices and IoT eUICCs						
SGP.25	Protection Profile - Embedded UICC for Consumer Devices	x				
SGP.24	RSP Compliance Process		x	x	x	x

eUICC for consumer devices						
SGP.21	Remote SIM Provisioning Architecture		x	x		
SGP.23-1 and SGP.26	RSP test specification and eSIM Test Certificates				x	
SGP.22	RSP Technical Specification		x	x		x
IoT eUICCs						
SGP.31	eSIM IoT Architecture and Requirements		x	x		
SGP.32	eSIM IoT Technical Specification		x	x		x
SGP.33-1 and SGP.26	eSIM IoT Test Specification				x	
eUICC for M2M						
SGP.01	eSIM M2M Architecture and Requirements		x	x		
SGP.02	eSIM M2M Technical Specification		x	x		x
SGP.11	eSIM M2M Test Specification				x	
SGP.05	SGP.05 M2M eSIM Protection Profile	x				

Table 3: GSMA eUICC specifications; functionality and security features

SGP.24 document usage is considered relevant as it describes exhaustive compliance to RSP process when it comes to functional and security product requirements as well as site security requirements. Moreover, SGP.24 is enforcing the use of a declaration template helping to establish full traceability and binding between product features that are about to be certified and product features that have actually been evaluated.

In the process of evaluating the GSMA eUICC specifications for their potential use as evidence in an EUCC certification, a detailed/comprehensive mapping and gap analysis have been undertaken to correlate each assurance class from the Common Criteria with specific clauses in the GSMA specification. A significant observation from this analysis is that the majority of the CC work units are fully addressed by the GSMA clauses, showcasing a robust alignment and compliance. While some requirements are only partially covered, necessitating potential supplementary measures or evidence from the developer, and a few might not be covered at all, it is noteworthy that the bulk of the criteria are comprehensively catered to by the GSMA specifications.

The following assurance components have been identified as potential candidates for re-use:

- ADV_FSP.4
- ADV_TDS.3
- AGD_OPE.1
- AGD_PRE.1
- ATE_COV.2
- ATE_FUN.1

The mapping tables presented in this annex will provide an in-depth breakdown of this alignment, elucidating the extent to which the GSMA specifications fulfil the Common Criteria assurance componenents listed here above.

In light of the preliminary mappings between the GSMA specifications and the Common Criteria requirements, there's a growing interest in substantiating these mappings with concrete and official evaluation. ENISA could explore in collaboration with EU certification bodies, the feasibility of conducting an EUCC evaluation to validate these mappings. While an initial assessment suggests that GSMA evidences align well with the Common Criteria, there is a consensus that a more formal validation is essential for their reuse within a CC certification. To this end, it is recommended to undertake a generic evaluation in accordance with CC/CEM by an EUCC or SOG-IS evaluation lab, specializing in the IT-technical domain of smart cards and similar devices. The culmination of this verified mapping could be an ECCG endorsed statement reflected through guidance or state-of-the-art documentation supporting the EUCC potentially.

A.3.3 Maintenance with partial re-evaluation

The Assurance Continuity EUCC maintenance process should be used in a both swift and cost-effective way, facilitating the extension of certificate validity to updated TOE versions. At present, this process is reserved for minor modifications. A "minor change" is defined as one that does not necessitate a formal evaluation by a lab, primarily because the TOE alteration evidently does not compromise its security functionality.

Should the TOE modification be deemed a "major change" (necessitating lab evaluation activities), then the re-evaluation procedure comes into play, culminating in the issuance of a fresh certificate. The generation of this new certificate mandates that all supporting evidence remains current. This introduces the potential for additional re-evaluation tasks, even if the modification is as minor as a bug fix. Such tasks could encompass the consideration of new interpretations, updates to site audits, comprehensive vulnerability analysis revisions, and more, potentially escalating both costs and time.

Proposed Enhancement:

We recommend broadening the scope of the maintenance process to accommodate maintenance coupled with partial re-evaluation. This partial re-evaluation would focus solely on the specific change, negating the need to update the untouched segments of the certification evidence, unlike a full re-evaluation. The outcome of such a maintenance process, paired with a partial re-evaluation, would be the extension or transfer of the existing certificate's validity to the revised TOE version. This refined process is especially apt for addressing bug fixes.

A.4 ADV_FSP.4

CC:2022 Work units	Tasks	Coverage level	Covered in	Rationale
Work unit ADV_FSP.4-1	The evaluator shall examine the functional specification to determine that the TSF is fully represented.	Full	Clause 5.1 in SGP.22	All TSFIs are listed: eUICC Interfaces, LPA to Server Interfaces
Work unit ADV_FSP.4-2	The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.	Full	The description of each interface contains the list of supported functions, description, command messages, parameters, data field, response messages ES6 (clause 5.4 in SGP.22) ES8+ (clause 5.5 in SGP.22) ES9+ (clause 5.6 in SGP.22) ES10a, 10b, 10c (clause 5.7 in SGP.22) ES11 (clause 5.8 in SGP.22)	For each interface, purpose, list of functions, method of use, parameters, actions are provided
Work unit ADV_FSP.4-3	The evaluator shall examine the functional specification to determine that the method of use for each TSFI is given.	Full	Idem	Idem
Work unit ADV_FSP.4-4	The evaluator shall examine the functional specification to determine the completeness of the TSFI	Full	Idem	Idem
Work unit ADV_FSP.4-5	The evaluator shall examine the presentation of the TSFI to determine that it completely	Full	Idem	Idem

	identifies all parameters associated with every TSFI.			
Work unit ADV_FSP.4-6	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.	Full	Idem	Idem
Work unit ADV_FSP.4-7	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all actions associated with every TSFI.	Full	Idem	Idem
Work unit ADV_FSP.4-8	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all error messages resulting from an invocation of each TSFI.	Full	Clause 5.2.6.2 in SGP.22	
Work unit ADV_FSP.4-9	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes the meaning of all error messages resulting from an invocation of each TSFI.	Full	Clause 5.2.6.2 in SGP.22	
Work unit ADV_FSP.4-10	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.	Not covered	Not covered	eUICC manufacturers often have their own mapping TSFIs-SFRs, It may be not useful to have it as a part of the public spec. It is to be provided by the developer as part of ADV_FSP or, or it could result from collaborative work with the evaluator, based on workshops.
Work unit ADV_FSP.4-11	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.	Not covered	Not covered	Idem
Work unit ADV_FSP.4-12	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.	Not covered	Not covered	Idem

Table 4: Mapping and gap analysis of GSMA eUICC specifications to CC ADV_FSP.4 components

A.5 ADV_TDS.3

CC:2022 Work units	Tasks	Coverage level	Covered in	Rationale
Work unit ADV_TDS.3-1	The evaluator shall examine the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.	Full	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	Decomposition into subsystems is described.

Work unit ADV_TDS.3-2	The evaluator shall examine the TOE design to determine that the entire TSF is described in terms of modules.	Partial	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	The module decomposition can be derived by the evaluator out of ADV_IMP
Work unit ADV_TDS.3-3	The evaluator shall examine the TOE design to determine that all subsystems of the TSF are identified.	Full	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	All components within the eUICC architecture have been identified and described
Work unit ADV_TDS.3-4	The evaluator shall examine the TOE design to determine that each subsystem of the TSF describes its role in the enforcement of SFRs described in the ST.	Not covered	Not covered	The evaluator can refer to the ASE and ADV_IMP to determine and understand how the subsystems enforce and implement the SFRs.
Work unit ADV_TDS.3-5	The evaluator shall examine the TOE design to determine that each SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-non-interfering.	Partial	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	The evaluator can refer to ADV_IMP to determine which subsystem is non-interfering with the SFRs.
Work unit ADV_TDS.3-6	The evaluator shall examine the TOE design to determine that interactions between the subsystems of the TSF are described.	Full	Covered in chapter 4.2 of SGP.21 and chapter 5 of SGP.22	All eUICC external and internal interfaces are listed and described.
Work unit ADV_TDS.3-7	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF and the modules of the TSF is complete.	Partial	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	The evaluator can derive the necessary evidence from the GSMA specifications and ADV_IMP to determine the mapping between the subsystems of the TSF and the modules of the TSF.
Work unit ADV_TDS.3-8	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF and the modules of the TSF is accurate.	Partial	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	Idem
Work unit ADV_TDS.3-9	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-enforcing module and relationship with other modules is complete and accurate.	Partial	Covered in chapter 4 of SGP.21 and chapters 2 and 5 of SGP.22	The evaluator can derive the necessary evidence from the GSMA specifications and ADV_IMP to ensure that the description of the purpose of each SFR-enforcing module and its relationship with other modules is

				complete and accurate.
Work unit ADV_TDS.3-10	The evaluator shall examine the TOE design to determine that the description of the interfaces presented by each SFR-enforcing module contain an accurate and complete description of the SFR-related parameters, the calling conventions for each interface, and any values returned directly by the interface.	Partial	Covered in chapter 4.2 of SGP.21 and chapter 5 of SGP.22	The evaluator can obtain the necessary evidence from the GSMA specifications and ADV_IMP to verify that the description of the interfaces provided by each SFR-enforcing module includes an accurate and complete account of the SFR-related parameters, the calling conventions for each interface, and any values directly returned by the interface.
Work unit ADV_TDS.3-11	The evaluator shall examine the TOE design to determine that SFR-supporting and SFR-non-interfering modules are correctly categorised.	Full	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	All modules within the eUICC architecture have been identified and described. The evaluator can refer to the descriptions provided by the GSMA specifications to categorize and determine which modules support SFRs and which are non-interfering with SFRs. he GSMA specifications also provide information on interactions between modules.
Work unit ADV_TDS.3-12	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-supporting or SFR-non-interfering module is complete and accurate.	Full	Covered in chapter 4 of SGP.21 and chapter 2 of SGP.22	Idem
Work unit ADV_TDS.3-13	The evaluator shall examine the TOE design to determine that the description of an SFR-supporting or SFR-non-interfering module's interaction with other modules is complete and accurate.	Full	Covered in chapter 4.2 of SGP.21 and chapter 5 of SGP.22	Idem
Work unit ADV_TDS.3-14	The evaluator shall examine the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the modules of the TSF described in the TOE design.	Partial	Covered in chapter 4 of SGP.21, chapters 2 and 5 of SGP.22 and ADV_IMP	The evaluator and developer can refer to the GSMA specifications, along with AD_FSP and ADV_IMP, to construct this mapping. This could be a collaborative effort between the developer and the lab, based on workshops.

Work unit ADV_TDS.3-15	The evaluator shall examine the TOE security functional requirements and the TOE design, to determine that all ST security functional requirements are covered by the TOE design.	Not covered	Not covered	eUICC manufacturers have often their own mappings of Modules to SFRs. It may not be beneficial to include these in the public specifications. These mappings should be provided by the developer as part of ADV_TDS, or it could result from collaborative work with the evaluator, based on workshops.
Work unit ADV_TDS.3-16	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.	Not covered	Not covered	Idem

Table 5: Mapping and gap analysis of GSMA eUICC specifications to CC ADV_TDS.3 components

A.6 ATE_COV.2, ATE_FUN.1

CC:2022 Work units	Tasks	Coverage level	Covered in	Rationale
ATE_COV				
Work unit ATE_COV.2-1	The evaluator shall examine the test coverage analysis to determine that the correspondence between the tests in the test documentation and the interfaces in the functional specification is accurate.	Full	In SGP.23-1: ES6: clause 4.2.2 ES8+: clauses 4.2.3 to 4.2.7, 4.3.7 to 4.3.11 ES9+: clauses 4.3.12 to 4.3.17, 4.4.21 to 4.4.26 ES10a: clauses 4.2.8, 4.2.9, 4.4.1, 4.4.2 ES10b: clauses 4.2.10 to 4.2.19, 4.4.3 to 4.4.12 ES10c: clauses 4.2.20 to 4.2.27, 4.4.13 to 4.4.20 ES11: clauses 4.4.27 to 4.4.29, 4.5.5, 4.4.6, 4.5.10 NOTE: SGP.26 contains test keys, valid test certificates and instructions for how to generate invalid	All interfaces are tested. For each interface at least one test case is associated

			certificates. All test keys and test certificates used in SGP.23-1 are bundled with SGP.26.	
Work unit ATE_COV.2-2	The evaluator shall examine the test plan to determine that the testing approach for each interface demonstrates the expected behaviour of that interface.	Full	Idem	Idem
Work unit ATE_COV.2-3	The evaluator shall examine the test procedures to determine that the test prerequisites, test steps and expected result(s) adequately test each interface.	Full	Idem	Idem
Work unit ATE_COV.2-4	The evaluator shall examine the test coverage analysis to determine that the correspondence between the interfaces in the functional specification and the tests in the test documentation is complete.	Full	Idem	Idem
ATE_FUN				
Work unit ATE_FUN.1-1	The evaluator shall check that the test documentation includes test plans, expected test results and actual test results.	Partial	In SGP.23-1: ES6: clause 4.2.2 ES8+: clauses 4.2.3 to 4.2.7, 4.3.7 to 4.3.11 ES9+: clauses 4.3.12 to 4.3.17, 4.4.21 to 4.4.26 ES10a: clauses 4.2.8, 4.2.9, 4.4.1, 4.4.2 ES10b: clauses 4.2.10 to 4.2.19, 4.4.3 to 4.4.12 ES10c: clauses 4.2.20 to 4.2.27, 4.4.13 to 4.4.20 ES11: clauses 4.4.27 to 4.4.29, 4.5.5, 4.4.6, 4.5.10 NOTE: SGP.26 contains test keys, valid test certificates	Test cases are described in terms of purpose, pre-conditions, excution steps, expected results

			and instructions for how to generate invalid certificates. All test keys and test certificates used in SGP.23-1 are bundled with SGP.26.	
Work unit ATE_FUN.1-2	The evaluator shall examine the test plan to determine that it describes the scenarios for performing each test.	Full	Idem	
Work unit ATE_FUN.1-3	The evaluator shall examine the test plan to determine that the TOE test configuration is consistent with the ST.	Full	Idem	
Work unit ATE_FUN.1-4	The evaluator shall examine the test plans to determine that sufficient instructions are provided for any ordering dependencies.	Full	Idem	
Work unit ATE_FUN.1-5	The evaluator shall examine the test documentation to determine that all expected tests results are included.	Full	Idem	
Work unit ATE_FUN.1-6	The evaluator shall check that the actual test results in the test documentation are consistent with the expected test results in the test documentation.	Not covered	Not covered	
Work unit ATE_FUN.1-7	The evaluator shall report the developer testing effort, outlining the testing approach, configuration, depth and results.	NA (Evaluator activity)		

Table 6: Mapping and gap analysis of GSMA eUICC specifications to CC ATE_COV.2 and ATE_FUN.1 components

A.7 AGD

CC:2022 Work units	Tasks	Coverage level	Covered in	Rationale
AGD_OPE				
Work unit AGD_OPE.1-1	The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.	Full	Clauses 3 'Procedures' 5 'Functions' in SGP.22	
Work unit AGD_OPE.1-2	The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the secure use of the available interfaces provided by the TOE.	Full	Idem	

Work unit AGD_OPE.1-3	The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the available security functionality and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.	Full	Idem	
Work unit AGD_OPE.1-4	The evaluator shall examine the operational user guidance to determine that it describes, for each user role, each type of security-relevant event relative to the user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.	Full	Idem	
Work unit AGD_OPE.1-5	The evaluator shall examine the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including, if applicable, operation following failure or operational error), their consequences and implications for maintaining secure operation.	Full	Idem	
Work unit AGD_OPE.1-6	The evaluator shall examine the operational user guidance to determine that it describes, for each user role, the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.	Not covered		
Work unit AGD_OPE.1-7	The evaluator shall examine the operational user guidance to determine that it is clear.	NA (Evaluator activity)		
Work unit AGD_OPE.1-8	The evaluator shall examine the operational user guidance to determine that it is reasonable.	NA (Evaluator activity)		
AGD_PRE				
Work unit AGD_PRE.1-1	The evaluator shall examine the provided acceptance procedures to determine that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.	Not covered		
Work unit AGD_PRE.1-2	The evaluator shall examine the provided installation procedures to determine that they describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.	Full	Clauses 3 'Procedures' 5 'Functions' in SGP.22	
Work unit AGD_PRE.1-3	The evaluator shall perform all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative procedures.	NA (Evaluator activity)		

Table 7: Mapping and gap analysis of GSMA eUICC specifications to CC AGD and ATE_FUN.1 components

ANNEX B – STATE OF THE ART PROTECTION PROFILES

This annex gives for each eUICC component the related candidate protection profiles. In addition, it identifies the gaps in current versions of these PPs. All this is conveyed in Table 8, which follows the color coding below:

Color code: Color coding for the representation of the gaps at the time of publication of this document.
No Gap PP is available, no gap has been identified.
Minor Gap A PP is available, a minor update would be required to bridge that gap.
Moderate Gap A PP is available, a moderate update would be required to bridge that gap.
Major Gap A PP is available, a major update would be required to bridge that gap.
Significant gap No PP available, new PP need to be created.

Figure 6 below shows the security evaluation protection profiles for each component within the eUICC.

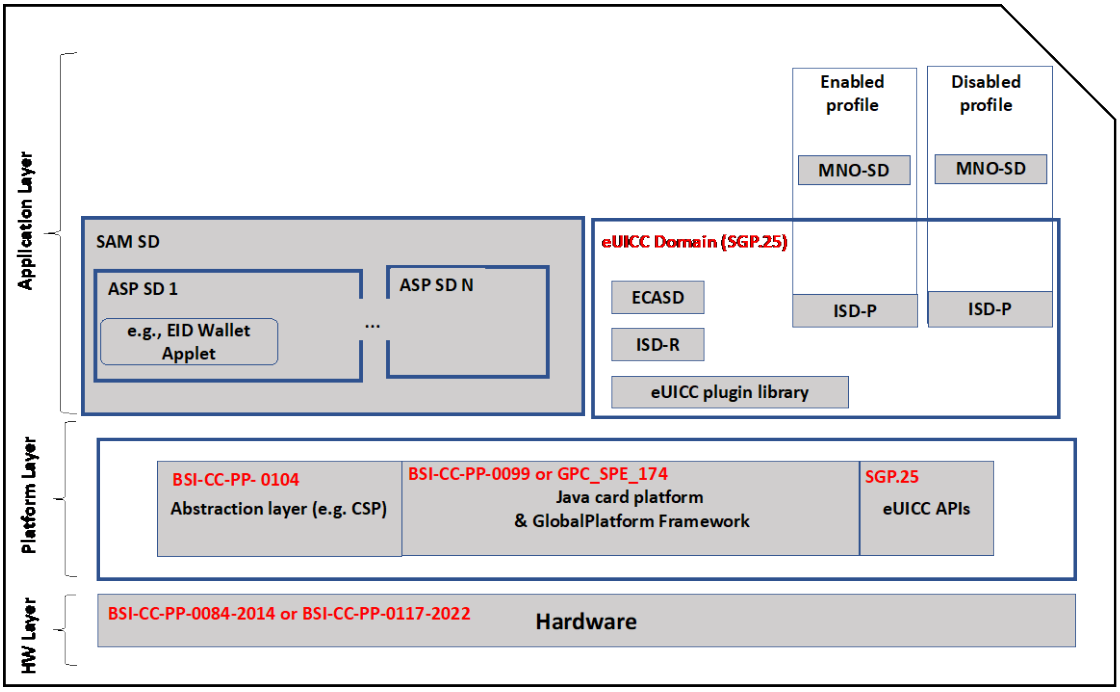

Figure 6: eUICC security evaluation protection profiles

PPs relevant for the eUICC certification are listed in Table 8. The column 'Gap' indicates the requirements on PP where further work by the 'Owner of the PP' is required.

Component	Protection Profiles required	Gap (what is missing from PP to be EUCC compliant), requirements on PPs	Owner of the PP	Note
eUICC hardware	**For a chip only BSI-CC-PP-0084[21]: Existing standard but revision needed** **or** **For a SoC BSI-CC-PP-0117[22]: Existing standard, no revision needed**	**The security target claiming conformance to BSI-CC-PP-0084 should be augmented with ALC_FLR.2.** **The new version of BSI-CC-PP-0084 should be augmented with ALC_FLR.2.**	**Eurosmart**	**Note:** Only the PP SoC BSI-CC-PP-0117-2022 supports ALC_FLR.2.
eUICC java card platform (JCP)	**BSI-CC-PP-0099[23]: Existing standard but revision needed**	**The security target claiming conformance to BSI-CC-PP-0099 should be augmented with ALC_FLR.2.**	**Oracle**	

21 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0084b_pdf.pdf?__blob=publicationFile&v=1, accessed May 2024.

22 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0117b_pdf.pdf?__blob=publicationFile&v=3, accessed May 2024.

23 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0099V2b_pdf.pdf?__blob=publicationFile&v=1, accessed May 2024.

		OR **The new version of BSI-CC-PP-0099 should be augmented with ALC_FLR.2.**		
eUICC java card platform (JCP) with GP framework	**GPC_SPE_174[24]: Existing standard but revision needed**	**The security target claiming conformance to GPC_SPE_174 should be augmented with ALC_FLR.2.** **The new version of GPC_SPE_174 should be augmented with ALC_FLR.2.**	**GlobalPlatform**	**Note:** The JCP with the GP framework should be certified according to GPC_SPE_174. However, in instances where not all SFRs of GPC_SPE_174 are implemented in the product, the author of the Security Target (ST) of the JCP is permitted to extend the ST by integrating the necessary elements (Assets, Threats, Objectives, SFRs) for the GP framework. In such cases, it is recommended to select these elements from GPC_SPE_174. This approach does not ensure full compliance with GPC_SPE_174 but ensures alignment with it, providing a balanced solution that accommodates the specific requirements of the GP framework while maintaining a connection to GPC_SPE_174.
eUICC RSP	**eUICC for CD and IoT: BSI-CC-PP-0100[25] (SGP.25): Existing standard but revision needed**	**The eUICC Common Criteria Protection Profile PP-0100 / SGP.25 shall be updated according to RSP specification version 3.0.** **The new version of the Common Criteria Protection Profile SGP.25 shall be EU CC or SOG-IS certified at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.** **The new version of SGP.25 should be augmented with ALC_FLR.2.**	**GSMA**	**Notes:** **For eUICC for CDs**: SGP.25 v1.0 (PP-0100) – Common Criteria Certified published version. It applies to version 2 of SGP21/22 SGP.25 v2.0 Non-Common Criteria Certified version to be published the end of Dec 2023. It applies to version 3 of SGP.21/22 Certified Common Criteria Version SGP.25 v2.1 – to be published Q1/Q2 2024. it applies to version 3 of SGP.21/22 **For IoT eUICCs:** SGP.25 v2.0 Non-Common Criteria Certified version to be published the end of Dec 2023. It applies to version 1 of SGP.31/32 Certified Common Criteria Version SGP.25 v2.1 – to be published Q1/Q2 2024. it applies to version 1 of SGP.31/32 ALC_FLR.2 and RSP v3.0 features will be part of SGP.25 v2 that will be certified at level EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

[24] https://www.commoncriteriaportal.org/files/ppfiles/CCN-CC-PP-5-2021.pdf, accessed May 2024.
[25] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0100b_pdf.pdf?__blob=publicationFile&v=1, accessed May 2024.

				For eUICCs for M2M, the SGP.05[26] applies.
		Currently, an on-TOE patch mechanism is already supported in GPC_SPE_174 (OS-update PP-module) and will be supported in SGP.25 v2.	**GP/GSMA**	**Note:** It is expexted that SGP.25 v2 will contain a PP-Module for on-TOE patch mechanism.
Secure application on mobile	**GSMA SAM requirements[27]** **GP SAM specification GPC_GUI_217[28]** **PP is needed**	**A Common Criteria Protection Profile for the SAM based on the GlobalPlatform specification shall be created and certified at EAL4 augmented with AVA_VAN.5 and ALC_DVS.2 following EUCC or SOG-IS scheme.**	**GlobalPlatform**	**Note**: There is no PP covering the SAM yet. SAM will be covered by a PP-Module in GPC_SPE_174. In cases where there is no full compliance with GPC_SPE_174, the author of the ST of the JCP with GP SAM is advised to integrate the PP-Module SAM from GPC_SPE_174 into the ST. This integration will help in aligning the ST with GPC_SPE_174, specifically addressing the aspects related to SAM, even when full compliance is not achievable. **Note:** GP Security WG will prepare the SAM PP-Module following the publication of SAM specifications
Cryptographic abstraction layer	**BSI-CC-PP- 0104[29]**	**The security target claiming conformance to BSI-CC-PP- 0104 should be augmented with ALC_FLR.2.** **The new version of BSI-CC-PP-0104 should be augmented with ALC_FLR.2.**	**BSI**	**Note:** A new BSI Technical Guideline TR-03181 CSP2 describing the requirements for the implementation of a CSP is now available[30].
	New standard needed (e.g., GP CSP standard for CSP) **Regarding the PP, three scenarios could arise:** **- Use of PP 0104 as it is (no impact of the spec on the PP)** **- Update of PP0104 according to the new spec or** **- New protection profile based on the new spec and using**	**New standard needed**	**GP**	**Note**: A new GP work item has been created to define the GP CSP specification: • Reference: GPC_SPE_230 • Name: GlobalPlatform Card Specification - Amendment N Cryptographic Service Provider. **Note:** The CSP shoud implement ZeroKnowledgeProof cryptographic APIs (for instance BBS+), in order to allow Privacy compliance

[26] https://www.gsma.com/esim/esim-m2m-specifications/, accessed May 2024.
[27] https://www.gsma.com/get-involved/working-groups/gsma_resources/sam-01-v1-1, accessed May 2024.
[28] https://globalplatform.org/specs-library/sam-configuration/?utm_source=BenchmarkEmail&utm_campaign=New_Publication_in_the_GlobalPlatform_Specification_Library_Available_for_Downlad_04162024&utm_medium=email, accessed May 2024.
[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0104b_pdf.pdf?__blob=publicationFile&v=1, accessed May 2024.
[30] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03181/TR-03181_node.html, accessed May 2024.

	as input the BSI-CC-PP- 0104			application usages in the coming year. if not, another SE may emerge with those technologies (market fragmentation).

Table 8: Specifications and PPs relevant for the eUICC certification

In addition, the following common rules adopted by the CCMS[31] after publication of CC:2022 shall be fulfilled by the eUICC PPs and STs:

- CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024.
- Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 will be accepted up to the 31st of December 2027.
- After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date.
- It is not recommended to perform Protection Profile evaluations on the basis of CC v3.1 after the beginning of 2024, as product evaluations on the basis of CC v3.1 will no longer be possible 6 months later.

From the hereabove list of CCMS rules, the following requirements have to be fulfilled by the eUICC PPs and STs:

- eUICC STs issued for the evaluation of eUICC products after 30th of June 2024 shall be based on CC:2022.
- New or updated eUICC PPs issued after the beginning of 2024 shall be based on CC:2022.
- Existing eUICC PPs shall be updated to be compliant with the CC:2022 no later than the 31st of December 2027.

[31] https://www.commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf, accessed May 2024.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu