TRUSTED CONNECTIVITY ALLIANCE

# Applying Security Assurance Principles Under the Cyber Resilience Act

A TCA Position Paper

# Contents

# 1. References

Selected informative references used in this document are included below:

| Standard / Specification | Definition |
|---|---|
| BSI-CC-PP-0084 | Security IC Platform Protection Profile with Augmentation Packages |
| BSI-CC-PP-0089 | Embedded UICC Protection Profile |
| BSI-CC-PP-0100 | Embedded UICC for Consumer Devices Protection Profile |
| BSI-CC-PP-0117 | Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile |
| CC | Common Criteria, ISO 15408 |
| CCDB-2007-11-001 | CCDB Guidance: Site Certification |
| CRA | Cyber Resilience Act |
| EMVCo | EMVCo Laboratory Accreditation Process |
| FS.04 | GSMA Security Accreditation Scheme for UICC Production - Standard |
| FS.05 | GSMA Security Accreditation Scheme for UICC Production - Methodology |
| FS.18 | GSMA Security Accreditation Scheme - Consolidated Security Requirements and Guidelines |
| GlobalPlatform | GlobalPlatform Functional Certification |
| SGP.02 | GSMA Remote Provisioning Architecture for Embedded UICC |
| SGP.05 | GSMA Embedded UICC Protection Profile |
| SGP.06 | GSMA eUICC Security Assurance Principles |
| SGP.07 | GSMA eUICC Security Assurance Methodology |
| SGP.11 | GSMA Remote Provisioning Architecture for Embedded UICC Test Specification |
| SGP.16 | GSMA M2M Compliance Process |
| SGP.22 | GSMA RSP Technical Specification |
| SGP.23-1 | GSMA RSP Test Specification for the eUICC |
| SGP.24 | GSMA RSP Compliance Process |
| SGP.25 | GSMA eUICC for Consumer and IoT Devices Protection Profile |
| SGP.32 | GSMA eSIM IoT Technical Specification |
| SGP.33-1 | GSMA eSIM IoT Test Specification for the eUICC |

# 2. Definitions

| Term | Definition |
|---|---|
| **eSIM** | eSIM is the generic term applied to devices and eUICCs that support Remote SIM Provisioning as defined by GSMA. |
| **eUICC** | A UICC which enables the remote and/or local management of profiles in a secure way that meet GSMA requirements for Remote SIM Provisioning and are certified in accordance with the GSMA compliance programme. The term originates from “embedded UICC”. |
| **Operator** | A mobile network operator or mobile virtual network operator; a company providing wireless cellular network services. An operator owns one or more international mobile subscriber identity (IMSI) ranges. |
| **Profile** | A combination of data and applications to be provisioned on a UICC or an eUICC for the purpose of providing connectivity to mobile networks. |
| **Remote SIM Provisioning** | The process of downloading, installing, enabling, disabling, and deleting a profile on an eSIM in accordance with GSMA Specifications. |
| **SIM** | A generic term for the application(s) that identify a subscriber and allow them to securely access a mobile network (e.g. 4G or 5G). SIM is sometimes used interchangeably with the term UICC or SIM card. |
| **SIM Card** | A SIM that has one of the physical plug-in form factors as defined by ETSI (i.e. plug-in, micro-SIM, nano-SIM). |
| **TRE (Tamper Resistant Element)** | A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data. |
| **UICC** | The platform, specified by ETSI, which can be used to run multiple security applications. These applications include the SIM for 2G networks, USIM for 3G, 4G and 5G networks, CSIM for CDMA, and ISIM (not to be confused with integrated SIM) for IP multimedia services. UICC is neither an abbreviation nor an acronym. |

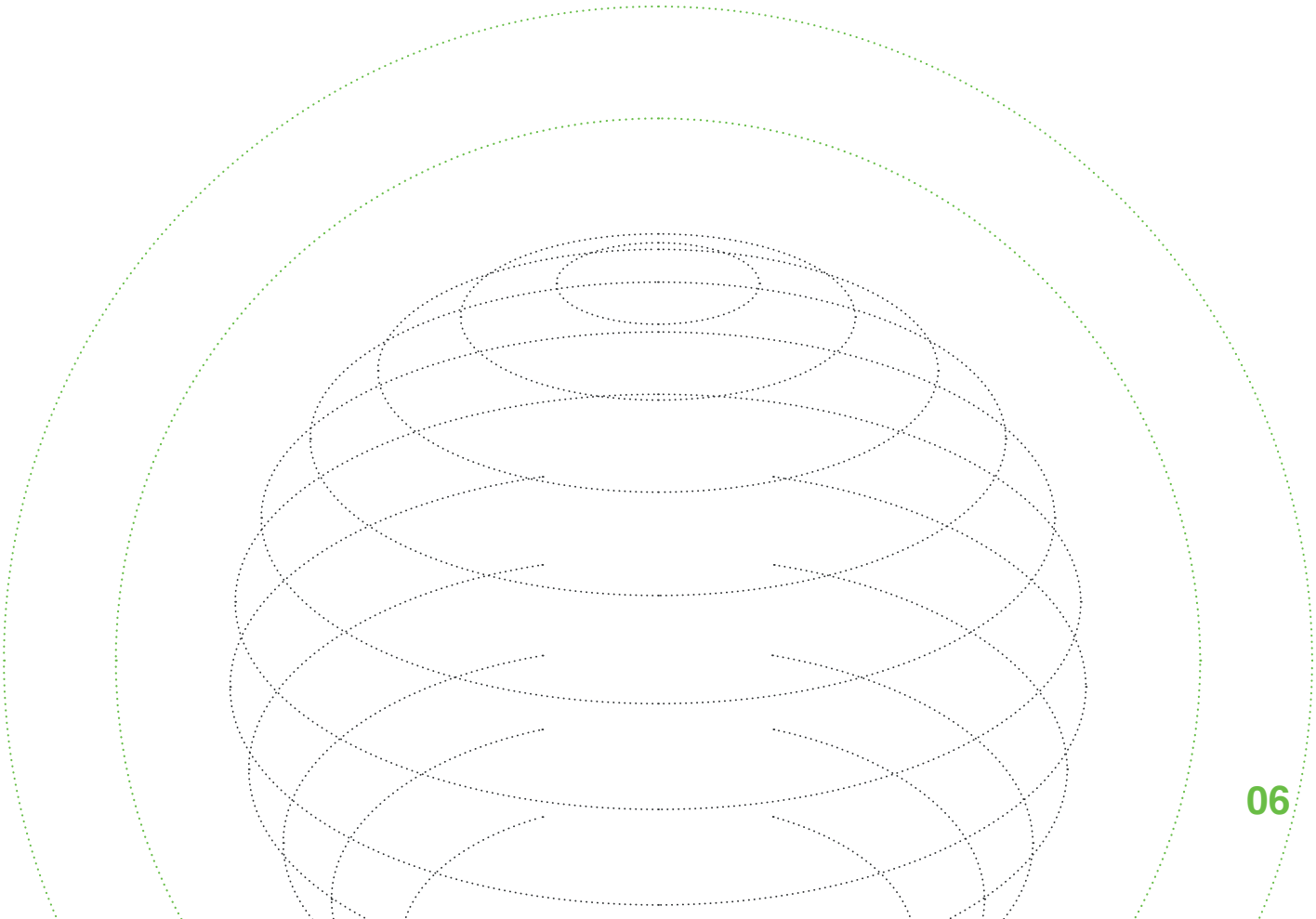
# 3. Scope of Document

TCA is actively exploring the implications of the global UICC market. This paper focuses specifically on how GSMA's eUICC Security Assurance (eSA) scheme could be integrated within the European Union's Cyber Resilience Act (CRA) conformity assessment framework for eUICC products, and could be considered also for the global UICC market.

TCA advocates that the requirements under the CRA should not be determined solely by the physical form factor of the UICC (e.g., plastic SIM cards, soldered chips, or embedded or integrated solutions). Instead, conformity assessments should be based on the core functionalities that the product delivers, particularly those that are critical to its intended use and associated risk profile.

Among these core functionalities, network authentication and user authentication are essential. Any product that performs these functions – regardless of whether it is a traditional SIM card, an eUICC, or another form – should be subject to the same level of security assessments under the CRA.

TCA looks forward to supporting the EU in defining practical and robust solutions for the full range of eUICC and UICC products. In line with this commitment, TCA will continue to publish recommendations covering any type of SIM product.



# 4. Executive Summary

**The European Union's Cyber Resilience Act (CRA) aims to safeguard consumers and businesses by introducing a stringent range of security requirements for all products with digital elements. Products must also undergo a conformity assessment before being placed on the market in order to demonstrate compliance with these requirements.**

As a global industry association whose members include leading providers of secure connectivity solutions for consumer, IoT and M2M devices – spanning Tamper Resistant Element (TRE) technologies including SIM, eSIM, integrated SIM, embedded Secure Element (eSE) and integrated Secure Element (iSE), as well as hardware and software provisioning and other personalisation services – Trusted Connectivity Alliance (TCA) applauds efforts to enhance cybersecurity across the connected world.

TCA welcomes the opportunity to demonstrate how the security capabilities defined in the GSMA Security Assurance (eSA) scheme – along with its supporting infrastructure – are well aligned with the cybersecurity requirements set out in international regulations such as the CRA. TCA is committed to supporting effective and efficient mechanisms for demonstrating such conformance.

TCA believes that the GSMA's established and proven eSA scheme represents a strong foundation and a promising reference for developing conformity assessment approaches tailored to UICC products. Building on the principles, methodologies, and assurance levels defined in eSA could enable a consistent and efficient path toward meeting CRA requirements across the UICC ecosystem.

**In this paper, TCA supports this position through:**

1. **A high-level overview of the GSMA eSA scheme and its benefits.**
2. **A detailed technical analysis of how the GSMA eSA scheme addresses essential security requirements defined within the CRA.**
3. **Recommended options for how the GSMA eSA scheme could be integrated within the CRA conformity assessment framework for eUICC products.**

# 5. Introduction: The Cyber Resilience Act and eUICC Products

The Cyber Resilience Act (CRA), published in the Official Journal of the European Union (EU) on November 20, 2024, aims to reduce vulnerabilities in digital products, ensuring manufacturers prioritise security throughout the product lifecycle. This regulation marks a significant step towards enhancing the overall cybersecurity landscape in the EU.

The CRA introduces horizontal cybersecurity requirements for all products with digital elements available on the market, ensuring a broad and consistent approach to cybersecurity. Based on the New Legislative Framework (which aims to improve the internal market for goods and strengthen conditions for placing products on the EU market, the CRA outlines a range of specific obligations for manufacturers, distributors, and importers to ensure these products meet stringent security standards and ensure ongoing protection against security threats,

For example, manufacturers must maintain cybersecurity essential requirements throughout the product's support period and ensure processes are in place for identifying, reporting, and mitigating vulnerabilities. CRA also mandates harmonised standards or requires the application of security schemes to ensure uniformity and high security levels.

**Understanding the Role of Conformity Assessments**

A key element of the CRA is that all products must undergo a conformity assessment before being placed on the market in order to demonstrate compliance with the CRA requirements. Conformity assessments are tailored to the risk level and required security, ensuring proportional and effective evaluation.

There are four categories of product under the CRA: Standard, Important – Class I, Important – Class II, and Critical. For products that are deemed to be 'critical', stricter rules apply and third-party assessment is the default option.

## 5.1 The CRA and the eUICC

The eUICC is a secure element which enables the remote and/or local management of profiles in a secure way that meet GSMA requirements for Remote SIM Provisioning and are certified in accordance with the GSMA compliance programme.

Put more simply, the eUICC is designed to host multiple profiles, which contain mobile network assets such as operator credentials and applications. Those profiles are used to provide secure, identifiable and authorised access for subscribers to mobile networks and services. The eUICC also provides mechanisms that enable profiles to be remotely provisioned, offering various benefits that have seen the eUICC emerge a critical component for consumer, IoT and M2M devices.

Due to its role in safeguarding sensitive data and ensuring secure communications, the eUICC falls within the scope of the CRA. Moreover, it is deemed to be a "critical product" that potentially requires third-party conformity assessment.

## 5.2 The CRA and the GSMA eUICC Security Assurance (eSA) Scheme

A key benefit of eSIM technology is that it is already supported by an advanced, mature infrastructure that promotes security and interoperability. A core element of this infrastructure is the **eUICC Security Assurance (eSA)**, which has been defined within the GSMA, the global association for the mobile industry, by various stakeholders and is recognised and trusted across the ecosystem.

eSA is an independent security evaluation scheme for eUICC software. It ensures that eUICC products meet rigorous security standards, providing assurance to mobile operators and consumers about the security of eUICCs. It also establishes trust for service providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secured against state-of-the-art attacks.

Importantly, eSA is based on the Common Criteria methodology (ISO 15408, which has been optimised to maximise process and time efficiencies to reflect device lifecycles.

The eSA scheme evaluates eUICCs against the security requirements defined in two possible Protection Profiles: Protection Profile BSI-CC-PP-0089 (SGP.05 and Protection Profile BSI- CC-PP-0100 (SGP.25).

These Protection Profiles have been developed by the GSMA and certified by the German Federal Office for Information Security (BSI). They outline security requirements for eUICCs used in consumer, IoT and machine-to-machine (M2M) devices, ensuring that eUICCs meet stringent security standards and providing a robust framework for protecting user data and maintaining secure communications.

# 6. Evaluating eSA Certification as a CRA Conformity Assessment Methodology

**This paper will use a structured approach to clearly outline and demonstrate how GSMA eSA certification can align with and support the CRA's cybersecurity mandates. Specifically, this document will evaluate how the GSMA eSA could serve as a conformity assessment methodology for the eUICC according to the structure outlined within "*Annex I: Essential Requirements*" of the CRA. This involves an analysis across three areas:**

1. **Manufacturer Risk Assessment:** How the eSA framework can be utilised to conduct comprehensive risk assessments by manufacturers, ensuring that all potential security threats are identified and mitigated.
2. **Essential Security Requirements Part I:** How the eSA can fulfil the initial set of essential security requirements, focusing on the foundational security measures that must be in place for compliance with the CRA.
3. **Essential Security Requirements Part II:** How the eSA addresses the second set of essential security requirements, with a particular emphasis on vulnerability handling, including the processes for identifying, reporting, and mitigating vulnerabilities throughout the product lifecycle.

# 7. GSMA eSA for: CRA Manufacturer Risk Assessment

**The obligations of manufacturers are described in the CRA within Article 13 under Chapter II: "*Obligations of Economic Operators and Provisions in Relation to Free and Open-Source Software.*" For an eUICC – which as noted above is considered as a critical product – this means:**

- **Rigorous Risk Assessment:** A comprehensive cybersecurity risk assessment must be performed and documented. This assessment should be updated throughout the product's lifecycle, typically reflecting a support period of at least five years.
- **Third-Party Assessment:** Evaluation is required by authorised third-party bodies to ensure compliance with cybersecurity standards before they can be marketed within the EU.
- **Vulnerability Management:** Manufacturers must implement robust mechanisms for identifying and addressing vulnerabilities. This includes ensuring that products are delivered without known exploitable vulnerabilities and maintaining a process for automatic updates and user notifications regarding security issues.

Importantly, manufacturers can use the eSA scheme to show compliance with these risk assessment requirements throughout the full product lifecycle, including the design and development, production, and support in field:

**During design and development:**

Products must be designed and developed with security in mind. eSA security certification is a process compliant with Common Criteria standards used by the manufacturers to assess the security of the products and the compliance of the development process.

The eSA certification scheme relies on several optimisations (as defined in SGP.07) that are allowed by the eUICC ecosystem, such as:

- Functional certification coverage by GSMA test suites SGP.11, SGP.23 and SGP.33-1 meeting the ATE_COV. 2, ATE_DPT.1, ATE_FUN.1, and ATE_IND.2 requirements. Compliance to these test suites is verified by GlobalPlatform functional certification.
- ALC_DVS.2 coverage by existing site certifications according to CCDB-2007-11-001 or EMVCo site audit, which are widely recognised across the industry.
- The GSMA SGP.02, SGP.22 and SGP.32 specifications describe the expected implementation of the remote provisioning feature and is considered to meet the AGD_PRE.1 and AGD_OPE.1 requirements.

**During production:**

- Supply chain vulnerabilities (e.g., components with hidden backdoors) are prevented by the mandatory use of hardware certified according to PP-0084 or PP-0117.
- Insider threats in manufacturing processes are covered by UICC production (SAS-UP) audits according to the following GSMA specifications: FS.18, FS.04 and FS.05.

**During product field life:**

- Risk management practices must be applied throughout the product lifecycle. Manufacturers shall provide security updates and disclose known vulnerabilities promptly.
- GSMA SGP.24 and SGP.16 define the compliance maintenance requirements and a product fast track update in case of vulnerability discovery. The mandatory update mechanism is covered by certification and the manufacturer is responsible for providing the update and to follow the certification maintenance process defined in SGP.24 and SGP.16.
- A process shall be established by manufacturers to identify and address vulnerabilities. In addition to the individual manufacturers' processes, it is worth considering that GSMA also manages a Coordinated Vulnerability Disclosure (CVD) programme with the eUICC in its scope. Although independent of the manufacturers' processes to address vulnerabilities, the GSMA CVD programme may potentially provide additional inputs to them. Finally, the SOGIS JIL Hardware-related Attacks Subgroup (JHAS) also manages hardware-related vulnerabilities for components used by eUICCs. It may also potentially provide inputs to the individual manufacturers' vulnerability management processes.

# 8. GSMA eSA for: CRA Essential Security Requirements Part I

**The below table outlines how the *"Essential Security Requirements Part I"* of the CRA are covered by a GSMA eSA security certification compliant to BSI-CC-PP-0100. A detailed analysis of the CRA requirements for BSI-CC-PP-0089 has not been conducted as it is anticipated that BSI-CC-PP-0089 products will migrate to BSI-CC-PP-0100 in the coming years. However, it is reasonable to expect that BSI-CC-PP-0089 covers the CRA requirements in the same way as BSI-CC-PP-0100.**

| Essential security requirement (CRA Annex I: Part I) | Assurance components in BIS-CC-PP-0100 v2 (Consumer + IoT) | Comments |
|---|---|---|
| (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks. | Fully covered by all components of PP-0100, in particular ASE, ADV, ALC and the security objectives defined in PP-0100 | |
| (2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall: | | |

| Essential security requirement (CRA Annex I: Part I) | Assurance components in BIS-CC-PP-0100 v2 (Consumer + IoT) | Comments |
|---|---|---|
| (2.a) be made available on the market without known exploitable vulnerabilities; | Fully covered by PP-0100 components AVA, ATE | |
| (2.b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state; | Fully covered by AGD_PRE for the first part.<br>Resetting the product to the original state is covered by SGP.22 and SGP.32 ES10c. eUICCMemoryReset. | |
| (2.c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them; | Partially covered by PP Module OS Update | As the eUICC is just a component in the device, the update process (e.g. the notification that an OS security update is released, the mechanism for users to allow or postpone download and installation) is managed by the device manufacturer. The eUICC manufacturer can just make available a security update to the device manufacturer when appropriate. |
| (2.d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access; | Fully covered by all components of PP-0100, in particular ASE, ADV, ALC, AVA and the security objectives of O.SECURE-CHANNELS | eUICC products are designed in a way that means unauthorised access is not possible. |
| (2.e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means; | Fully covered by all components of PP-0100, in particular ASE, ADV, ALC, AVA and the security objectives of O.SECURE-CHANNELS and O.DATA-CONFIDENTIALITY | |

| Essential security requirement (CRA Annex I: Part I) | Assurance components in BIS-CC-PP-0100 v2 (Consumer + IoT) | Comments |
|---|---|---|
| (2.f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions; | Fully covered by all components of PP-0100, in particular ASE, ADV, ALC, AVA and the security objectives of O.SECURE-CHANNELS and O.DATA_INTEGRITY | |
| (2.g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation); | Covered by ATE, AVA. | According to SGP.21/22 and SGP.31/32, any data which could be used to identify an individual SHALL be treated as personal data and subject to local regulations (e.g., the EID, ICCID, IMEI, IMSI etc).<br>The RSP Session SHALL prevent sending IMEI and EID information to a non-authenticated RSP Server. |
| (2.h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks; | Some attacks might trigger a protection that terminates the eUICC. | It is a well-established practice that protection of the asset is more important than the availability of the component function.<br>Such practice is in line with Requirement 1 in the CRA Essential Security Requirements: it is assumed in-fact that there are cases in which protections that terminate the eUICC are the appropriate measure based on the risk. |
| (2.i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks; | | The eUICC is responsible for the network authentication of a device. The ecosystem is intentionally defined in a way that means a device does not get connected if the eUICC is not available. However, mobile devices will always provide a possibility to initiate emergency calls and receive emergency messages. |

| Essential security requirement (CRA Annex I: Part I) | Assurance components in BIS-CC-PP-0100 v2 (Consumer + IoT) | Comments |
|---|---|---|
| (2.j) be designed, developed and produced to limit attack surfaces, including external interfaces; | Fully covered by all components of PP-0100, in particular ASE, ADV, ALC and the defined security objectives of PP-0100. | |
| (2.k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques; | Partially covered by ALC_FLR when incidents occur after product delivery. | If an incident occurred on a eUICC, it is possible for operators to decline delivering a profile to that eUICC based on their security policies, for example. |
| (2.l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user; | In terms of risk-based cybersecurity, this requirement is not relevant for eUICCs. However, in the eSIM ecosystem this requirement is partially covered by "Notifications" defined in SGP.21/22 and SGP.31/32. | The "Notification" mechanism allows the eUICC / mobile device to securely notify an operator that the user manages (i.e. enables, disables or deletes) their telecom profile.<br><br>Nevertheless, the Notification mechanism:<br>1. Is based on "best effort", i.e. the notification message, although cryptographically protected, is not based on a reliable protocol<br>2. Has an opt-out mechanism managed by the Telecom Operator providing the Profile/subscription, |
| (2.m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner. | Resetting the product to the original state is covered by SGP.22 and SGP.32 ES10c. eUICCMemoryReset.<br><br>Secure transfer of subscriptions between eUICCs is covered by SGP.22 and SGP.32 Device Change feature. | |

# 9. GSMA eSA for: CRA Essential Security Requirements Part II

**The below table outlines how the *"Essential Security Requirements Part II"* of the CRA are covered by a GSMA eSA security certification compliant to BSI-CC-PP-0100. Again, a detailed analysis of the CRA requirements for BSI-CC-PP-0089 has not been conducted as it is anticipated that BSI-CC-PP-0089 products will migrate to BSI-CC-PP-0100 in the coming years. However, it is reasonable to expect that BSI-CC-PP-0089 covers the CRA requirements in the same way as BSI-CC-PP-0100.**

| Essential security requirement (CRA Annex I: Part II) | Assurance components in BSI-CC-PP-0100 v2 | Comments |
|---|---|---|
| Manufacturers of products with digital elements shall: | | |
| (1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products; | ALC_FLR.2 Flaw reporting procedures (suggested).<br>ALC_CMC CI list provides a BoM. | GSMA SGP.07 defines the security evaluation process for eSIM products. This process produces vulnerability analysis, penetration test plan and test results.<br>All source code is provided to the evaluation laboratory as part of an AVA_VAN.5 evaluation.<br>A Configuration Item list, including all source code files, is also provided |
| (2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates; | PP Module OS Update enables this.<br>Updates are normally provided by the eUICC manufacturer and deployed by the mobile device manufacturer. | GSMA SGP.25 includes Annex A to address the security requirements related to the eUICC OS Update capability. |

| Essential security requirement (CRA Annex I: Part II) | Assurance components in BSI-CC-PP-0100 v2 | Comments |
|---|---|---|
| (3) apply effective and regular tests and reviews of the security of the product with digital elements; | | GSMA SGP.06 covers risk management of the eSA Scheme so that the corresponding periodic review:<br>• Analyse potential security flaws not covered by the scheme and manage the evolution of the scheme, the PP-0100 and the corresponding list of attacks.<br>• Analyse and mitigate security issues reported by the GSMA Certification Body.<br>These objectives are met by the activities of the GSMA Fraud and Security Group (FASG) and CVD programme.<br>GSMA FASG constantly monitors developing attacks, while the GSMA CVD programme provides a framework for security researchers to provide their findings without prejudice towards the manufacturers.<br>JHAS group maintains a catalogue of attacks and evaluation labs scan for emerging attacks as part of their normal working practice.<br>The reviews are then initiated by new attack methods rather than a specific timeframe. This approach ensures that monitoring stays closely aligned with the current state-of-the-art in attack methods. |
| (4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch; | ALC_FLR.2 Flaw reporting procedures (suggested). | The GSMA CVD programme provides such a framework.<br><br>Additionally, GSMA SGP.25 includes the corresponding assurance requirement augmentation as optional but suggested.<br><br>As defined in GSMA SGP.24, declarations allow updates of the product to fix errors or vulnerabilities which are discovered on already deployed products. Lab review of the change is a prerequisite.<br><br>Lab review of vulnerability fixes to ensure they are adequate means the potential vulnerability is disseminated within the security assurance ecosystem. |

| Essential security requirement (CRA Annex I: Part II) | Assurance components in BSI-CC-PP-0100 v2 | Comments |
|---|---|---|
| (5) put in place and enforce a policy on coordinated vulnerability disclosure; | | The GSMA CVD programme provides such a framework. This vulnerability disclosure is limited to the persons that needs to know in client to avoid any counterproductive effect before the mitigation plan is defined and run.<br>This is done on a case-by-case basis, potentially enforced by the contracts. |
| (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements; | ALC_FLR.2 Flaw reporting procedures (suggested). | The GSMA CVD programme provides such a framework.<br><br>Additionally, GSMA SGP.25 includes the corresponding assurance requirement augmentation as optional but suggested.<br><br>This is done on a case-by-case basis, potentially enforced by contracts. |
| (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner; | PP Module OS Update. | CRA mandates that, where applicable, the Security Target must include the PP module 'OS Update' of BSI-CC-PP-0100, which defines the Security Objectives for the eUICC update process.<br><br>Distribution of such updates would be the responsibility of the device manufacturer. However the security of the update process is assured by the evaluation of 'OS Update' module since GSMA SGP.25 includes Annex A to address the corresponding security requirements. |
| (8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken. | PP Module OS Update. | This is the existing common practice for eUICC. It is done on a case-by-case basis, potentially enforced by the contracts.<br><br>The requirement refers to the free-of-charge nature of updates. This aspect refers more to a commercial agreement topic with the client than a cybersecurity-related one. |

## 9.1 Vulnerability Handling Requirements supported by GSMA eUICC Functional and Security Compliance

**Further to the analysis outlined above, this section provides further information on how vulnerability handling requirements are addressed by the GSMA eSA scheme – as well as broader GSMA compliance ecosystem.**

The requirements for initial Vulnerability Analysis are fulfilled by the eSA scheme, which requires a Common Criteria AVA_VAN.5 analysis of the product performed by an approved third-party testing laboratory. This means that all source code is made available and subject to analysis and testing against 'state-of-the-art' attack techniques at the time of evaluation.

In accordance with the BSI-CC-PP-0100 (where a product provides the means to update the OS), the Security Target includes the PP Module 'OS Update.' This defines the security objectives for securely loading and activating the OS updates, including Target of Evaluation (TOE) identification changes and managing interruptions to the update process.

### Assurance Continuity

The GSMA eSA scheme provides a 'maintenance' process which allows for the updated functionality to be assessed against any identified vulnerability and the updated TOE to be included in the scope of the original certificate, retaining the same validity period (five years from initial issuance).

The validity of a certificate can be extended by a 'recertification.' This means the product will be subject to the current 'state-of-the-art' attack techniques.

As with the initial evaluation, all assurance continuity processes require that the evaluator has complete access to the relevant source code.

### Vulnerability Reporting

The GSMA CVD programme provides an established framework for security researchers to disclose vulnerabilities to the GSMA ecosystem. Further to the GSMA-CVD, GSMA encourages and supports member companies to run their own vulnerability disclosure programmes, with guidance on how they can be operated. This encourages universities and ethical hacker groups to engage with the GSMA and manufacturers directly, ensuring that products are subject to ongoing attack development.

### Support Period

The CRA stipulates that manufacturers should have a defined period of support aligned with the expected lifetime of the product. Five years is suggested as the baseline, with justification required for a shorter support period and an expectation that products with a longer expected life should be supported for that time. The regulation suggests that the European Commission should manage a harmonised approach to support periods for all digital products, based on statistical analysis of average support periods. GSMA is well placed to provide guidance on the support periods to ensure that there are no variations across member states and jurisdictions.

# 10. Recognising GSMA eSA as a Conformity Assessment Methodology for the CRA

**In the above sections, it is proven that the GSMA eSA scheme would be a robust method for the conformity assessment of the CRA requirements, particularly when used in conjunction with the eUICC Common Criteria Protection Profile BSI-CC-PP-0100. This combination effectively meets the essential security requirements of the CRA, while offering a streamlined approach to ensuring compliance.**

There are two potential pathways to integrate GSMA eSA within the framework of the CRA conformity assessment:

- **Option 1:** Leverage all the optimisations developed for the GSMA eSA for the emerging EU5G scheme, which is currently under development by the European Union Agency for Cybersecurity (ENISA). This approach would result in an optimised EUCC (EU Common Criteria) scheme that aligns with the standards set by GSMA eSA for the eUICC.
- **Option 2:** Considering the high level of security it delivers, evaluate the eSA assessment methodology to align with the EC's conformity module approach – with specific reference to Module H (design and production phase) – and meet the corresponding requirements. Additionally, propose GSMA to be established as an EU-based Notified Body responsible for carrying out conformity assessment.

While both options present viable paths forward, TCA believes Option 2 is the best approach as it builds on the validated eSA scheme with its Common Criteria methodology to prove the high level of security for eUICC products in an efficient manner.

# 11. Conclusion

From the very beginning, the eUICC specifications have been developed with the clear goal of fulfilling the highest security standards. The eUICC components have been specified to be resistant to attacks with a high attack potential in the terms of Common Criteria (AVA_VAN.5). Therefore, it is not surprising that the essential security requirements defined within the CRA are already well covered by the eUICC specifications.

In addition, the GSMA has created with the GSMA eSA scheme a Common Criteria methodology to prove the high level of security for eUICC products in an efficient manner. This approach has been validated since the start of the GSMA eSA scheme by the many security certifications achieved.

As is clearly and extensively demonstrated in this paper, the GSMA eSA is capable of proving conformance to the CRA requirements for eUICC products and it should be recognised as such.

Looking ahead, TCA is committed to driving forward the necessary activities to maintain the high level of eUICC security and to define efficient and reliable mechanism for demonstrating the conformance to international security regulations, including the CRA.

# 12. About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global industry association working to enable trust in a connected future.

The organisation evolved from the SIMalliance, reflecting the continued expansion of the global SIM industry and the need for broader collaboration. Its members are leading providers of secure connectivity solutions for consumer, IoT and M2M devices. This spans Tamper Resistant Element (TRE) technologies including SIM, eSIM, integrated SIM, embedded Secure Element (eSE) and integrated Secure Element (iSE), as well as hardware and software provisioning and other personalisation services.

TCA members are:

Giesecke+Devrient
IDEMIA
life.augmented
THALES
Valid
NXP
card centric
COMPRION
东信和平 EASTCOMPEACE
Kigen
Linxens
monty mobile THE ART OF TELECOM
RedteaMobile
TRASNA