GSMA eUICC SECURITY ASSURANCE SCHEME STANDARD TERMS AND CONDITIONS ("eSA STCs")

1 eSA's OBJECTIVES

1.1 The GSMA eUICC Security Assurance Scheme ("eSA") is an independent security evaluation scheme for evaluating embedded UICCs (eUICCs) against the provisions of Protection Profiles for eUICCs (currently PP-0089 [1] and PP-0100 [2]).

1.2 The eSA aims to establish trust for Service Providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secure against state-of-the-art attackers. The eSA is based on the Common Criteria methodology ISO15408 [3], optimised for GSMA compliant eUICCs.

1.3 The eSA is operated in accordance with the current:
(i) the provisions of ISO17065 [4].
(ii) SGP.06 eUICC Security Assurance Principles [5]; and
(iii) SGP.07 eUICC Security Assurance Methodology [6];

1.4 The eSA owner is the GSMA.

1.5 The eSA includes a certification function with the Certification Body (CB) role.

2 REFERENCE

Ref	Doc Number	Title
[1]	[SGP.05]	Embedded UICC Protection Profile, also published by BSI as BSI-CC-PP-0089-2015
[2]	[SGP.25]	RSP eUICC for Consumer Device Protection Profile, also published by BSI as BSI-CC-PP-0100-2018
[3]	[ISO15408]	The Common Criteria for Information technology — Security techniques — Evaluation criteria for IT security
[4]	[ISO17065]	Conformity assessment — Requirements for bodies certifying products, processes, and services
[5]	[SGP.06]	eUICC Security Assurance Principles
[6]	[SGP.07]	eUICC Security Assurance Methodology;
[7]	[AA.35]	GSMA Procedures for Industry Specification
[8]	[AM]	JIL Attack Methods for Smartcards and Similar Devices
[9]	[AP]	JIL Application of Attack Potential to Smartcards

3 eSA's FRAMEWORK

3.1 Each party to participate in the eSA ("eSA Participant(s)"), i.e.
- the CB;
- each Licensing Laboratories (i.e. security evaluation laboratory licensed by a GSMA CB to perform eUICC security evaluations);
- each EUM (i.e. UICC manufacturers);

shall be bound by these eSA STCs.

3.2 Before commencing work on or being recipient of any services associated with the eSA, each eSA Participant needs to have individually:
(i) paid their License and Administration Fee set out in Annex A ("eSA Fee") in full, and
(ii) provide the GSMA with a signed and dated copy of the declaration by two duly authorized signatories set out in Annex B ("Registration")

3.3 In case of any conflict with any third party terms and conditions or underlying agreements associated with the eSA, these eSA STCs shall prevail.

3.4 The main scope GSMA eUICC Security Assurance eSA is set out in the most current version of SGP.06 eUICC Security and SGP.07 eUICC Security Assurance Methodology.

3.5 In accordance with SGP.06 eUICC Security Assurance Principles:

(i) eSA oversight shall be performed by a GSMA Advisory Panel. The GSMA Advisory Panel shall be governed by the provisions of AA.35 GSMA Procedures for Industry Specification [7].
For the purpose of the eSA, the eSIM Group shall be deemed the GSMA Advisory Panel.

(ii) disputes between eSA Participants shall be subject to the Appeal process set out in Section 10 of AA.35 [7]; and

(iii) eSA monitoring shall be performed by GSMA.

4 eSA PARTICIPANT'S REPRESENTATIONS AND WARRANTIES

4.1 The eSA Participants hereby agree, undertake, represent and warrant that they will adhere to, execute and enforce all the processes, tasks and details defined and prescribed within SGP.06 and SGP.07.

5 RESPONSIBILITIES OF THE PARTICPANTS OF THE eSA

5.1 *CBs*

The CB is the certification body for the eSA responsible for gaining and maintaining ISO17065 [4] for the eSA, including identifying necessary updates to the eSA documentation to align with ISO17065 [4] expectations.

The CB is responsible for:

- Initial quotation to EUM based on Submission phase activities
- Participate in the evaluation meetings and review documentation from Licensed Laboratory and EUM during evaluation phase
- Certification activities for the eSA
- Licensing laboratories for the eSA (according to the eSA defined criteria)
- Alignment of Licensed Laboratories to ensure a common approach to evaluations performed under the eSA according to SGP.06 and SGP.07 and latest JIL guidance ([8] and [9]).
- Maintenance of certificate status in accordance to the ISO17065 requirements, especially when informed of non-compliance to the requirements, and informing GSMA of such changes.

5.2 *Licensing Laboratories*

The Licensing Laboratories are the security evaluation laboratories licensed by a CB (fulfilling the eSA requirements and defined criteria) to perform eUICC security evaluations for the eSA.

The Licensed Laboratory is responsible for:

- Submission activities together with the EUM
- Evaluation activities for the eSA
- Participate in evaluation meetings and present documentation to CB during evaluation phase according to SGP.06 and SGP.07 and latest JIL guidance ([8] and [9]).
- Create and signed final Evaluation Technical Report after the evaluation phase
- Informing GSMA, the CB promptly when the eUICC product(s) are known to not be compliant to the requirements (such as known vulnerabilities).

5.3 *EUMs*

EUMs are the eUICC Manufacturer that has developed an eUICC product(s) for under evaluation and certification under the eSA.

The EUM is responsible for:

- Drafting the Security Target (ST)
- Submission activities together with the Licensed Laboratory

- Make all EUM evaluation documentation available for the GSMA CB to review during the evaluation meetings
- Optionally participate in evaluation meetings to assist on the presentation of the evaluation documentation to CB
- Informing GSMA, the CB and the lab promptly when the eUICC product(s) are known to not be compliant to the requirements (such as known vulnerabilities).

6 GRANT OF CERTIFICATION

6.1 The eSA Certificate it is a Co-branded certificate authorised by GSMA to be issued by CB, containing logos and signatures from both organisations as well as eSA Certificate ID and other relevant information related to the eUICC product, the EUM information and the Licensed Laboratory that run the evaluation.

6.2 The eSA Certificate ID is a digital or numeric mark that represents a reference assigned to certified eSA products from a specific EUM Company by GSMA and CB.

6.3 The following steps need to be adhered to in order to receive the eSA Certificate:

(a) Upon acceptance of these STC by the respective EUM and following receipt of all the necessary EUM documentation to the satisfaction GSMA, the GSMA will issue to the EUM a confirmation of enrolment in the GSMA eSA Scheme ("GSMA eSA Enrolment Confirmation").

(b) Upon receiving the GSMA eSA Enrolment Confirmation, the EUM will have to successfully complete the phases set out within SGP.06 eUICC Security Assurance Principles [5] and SGP.07 eUICC Security Assurance Methodology [6] to the satisfaction of the CB and GSMA.

(c) Upon the successful completion of the above phase in Clause 6.1(b) by the EUM, the CB and GSMA will issued the EUM with an eSA Certificate.

(d) The decision by the CB to issue the eSA Certificate are taken as is by the GSMA.

(e) The EUM hereby acknowledges and agrees that the GSMA shall have no liability and the EUM shall have no further resource against the GSMA or the CB for the decisions of the GSMA to issue or not issue the eSA Certificate.

6.4 After the eSA Certificate has been issued by the CB as authorise by GSMA, the GSMA will display:

(i) the eSA Certificate
(j) the EUM eSA Certificate holder company's name,
(k) associated product name; and
(l) eSA Certificate expiration date

on the GSMA eSA Products Database and on the GSMA eSA Web Page.

6.5 The EUM hereby grants the GSMA a perpetual, fully paid up and irrevocable licence to use, publish or display the eSA Certificate and associated EUM eSA Certificate holder company's information at any times as the GSMA thinks fit.

7 GSMA THIRD PARTY RIGHTS, WARRANTIES & LIMITATION OF LIABILITIES

7.1 Notwithstanding any provisions in any of any (underlying) contracts between the CB, any Licensing Laboratories or EUMs associated with the eSA:

(i) each of the above parties agree that the GSMA may enforce any rights and obligations in relation to the eSA and provisions associated with it against the above parties irrespective of the exclusion of the Contracts (Rights of Third Parties) Act 1999 in their contracts associated with the eSA;

(ii) all deliverables, information, materials, services and/or other activities performed, undertaken or provided by the GSMA in association with the eSA are provided "as is" and without any warranty of any kind. All GSMA warranties in association with the eSA, whether expressed or implied, or statutory, including without limitation any implied or other warranties of merchantability, fitness for a particular purpose, non-infringement, quality, accuracy, completeness, title or quiet enjoyment are expressly disclaimed and excluded by the Parties;

(iii) the GSMA does not give any warranty that the goals of the eSA will be achieved. The CB, any Licensing Laboratories or EUMs, enters into this MoU without reliance on any representation and/or warranty of

the GSMA and all such GSMA representations and/or warranties are, to the greatest extent permitted by applicable law, hereby disclaimed;

(iv) each of the above parties acknowledge and agree that the eSA, its evaluation, certification and any associated matter are solely for the benefit of the EUM and for their information only. The ASSOCIATION shall not be liable for any third-party reliance on or claim against the eSA, its evaluation, certifications and/or any associated matter;

(v) in the case of any alleged third-party reliance on or claim against the eSA, evaluation, certification and/or any associated matter, the EUM will fully and finally settle such matter (irrespective if brought against the GSMA) from its own funds without any recourse to the GSMA;

(vi) In the event that the GSMA is nonetheless deemed liable in contract, tort, or for any breach of statutory duty in relation to the eSA, the aggregate liability of the GSMA for all claims associated with the eSA shall not exceed a maximum of one thousand Euro (€1,000) for all related claims associated breach. GSMA shall not be liable to CB, any Licensing Laboratories or EUMs for any special, direct, indirect, incidental, exemplary, punitive or consequential damages and expenses (collectively, "Losses"), whether occasioned by the act, breach, omission, default or negligence of the GSMA, its employees and contractors and sub-contractors. Losses shall include without limitation, lost profits, lost savings, economic loss, business interruption, lost business information, loss of use or data, loss of savings or anticipated savings, loss of investments, loss of goodwill, loss of reputation or cost of capital or loss or extra administrative cost whether or not foreseeable, flowing from any one event or series of connected events arising out of or in connection with this eSA howsoever that liability arises, including without limitation, breach of contract, tort, non-fraudulent misrepresentation or arising from statute, indemnity or otherwise. Notwithstanding the forgoing, nothing in this eSA shall exclude or limit the liability of either party for death or personal injury caused by negligence or for fraud; and

(vii) the CB, any Licensing Laboratories or EUMs shall jointly and severable be liable any Fees and reasonable cost and expenses incurred by the GSMA as a result of any cancellation or delay of an evaluation, non-payment or delay of payment of Fees or breach of any provisions of the eSA by any of them.

7.2 The eSA Participants herewith acknowledge and agree that if any of them breaches the terms and conditions of the eSA, the GSMA may choose to seek injunctive relief in addition to any other rights and remedies the GSMA may have.

8 INTELLECTUAL PROPERTY

8.1 Save in the case, as expressly stated below, nothing in these eSA STCs shall affect, or be construed as affecting, any intellectual property rights of the GSMA or any eSA Participants. For the avoidance of doubt, eSA Participants are not entitled to use the GSMA marks for the purpose of eSA unless expressly authorised by the GSMA in writing

8.2 Each eSA Participant grants the GSMA an irrevocable and fully paid up license to use any information received in relation to the eSA Certificate to provide services and products associated with:

(i) the prevention of fraud; and
(ii) the enhancement of telecommunication security;

for the benefit of the industry.

9 CONFIDENTIALITY

9.1 For the purposes of this eSA, "Confidential Information" shall include all information whatever its nature relating to the GSMA, the CB, any Licensing Laboratories or EUMs which has been or is disclosed by one party the "Disclosing Party") to the other party (the "Receiving Party") or to which the Receiving Party has been given access, whether in oral, written, graphic, photographic, digital, binary, electronic or paper or in any other form whatsoever, howsoever stored, whether or not pursuant to discussion with the Disclosing party;

9.2 The obligations set out in Clause 9.1 do not apply to;

(i) Information provided under Clause 8.2 to the GSMA, as the GSMA thinks fit.

(ii) Confidential information, which at the time of disclosure to the Receiving Party is within the public domain;

(iii) Confidential information which after such disclosure comes into the public domain, otherwise than by reason of a breach of any of the undertakings in Clause 6.3 below; or

(iv) Confidential information which was lawfully within the possession of the Receiving party prior to its being furnished to the Receiving party by or on behalf of the Disclosing party as evidenced by the written records of the Receiving Party provided that such information was not subject to obligations of confidentiality separate from those contained herein.

9.3 In consideration of Confidential Information being made available to the Receiving Party, the Receiving party will procure that:

(i) Use of the Confidential Information by the Receiving Party will only occur during the term of this eSA and for purposes relating to this eSA;

(ii) The Receiving Party will treat and safeguard as private and confidential all the Confidential Information received at any time by the Receiving Party from the Disclosing Party. This obligation shall remain in force after expiration or termination of this eSA;

(iii) The Receiving Party shall not, at any time without the prior written consent of the Disclosing Party, disclose or reveal the confidential information to any other person or party whatsoever, other than officers, employees, advisors and agents of the Receiving Party or authorised third parties who are required in the course of their duties to receive and consider the same and who shall be required by the Receiving Party to observe the same restrictions on the use and disclosure of the Confidential Information as are contained in this confidentiality clause.

(iv) The Receiving Party shall make known without delay to general counsel/head lawyer of the Disclosing Party, any improper disclosure on the part of any employee or customer of the Receiving Party or any other person, which comes to the knowledge of the Receiving Party.

9.4 Notwithstanding the confidentiality obligations set forth in this Clause 9, the GSMA shall be authorized to disclose fully-anonymized examples of poor business practice derived from Evaluation Technical Reports prepared pursuant to this eSA, solely for the following limited purposes:

(i) To provide guidance to participating suppliers through the selective disclosure of examples of poor business practices which can lead to unsuccessful evaluation and certification results, and

(ii) To demonstrate to GSMA members the benefits of implementing best practices with respect to the eSA.

10 TERM AND TERMINATION

10.1 GSMA at its sole discretion without any further recourse by the CB, or any Licensing Laboratories or EUMs may terminate:

(a) this eSA at any time; and

(b) the participation of the CB or any Licensing Laboratories or EUMs:

(i) immediately upon written notice if any of them files a petition in bankruptcy, becomes insolvent, goes into receivership or dissolves; and

(ii) immediately upon written notice for breach any substantial or material obligation or a continuing breach of this eSA where such default or breach remains uncorrected for a period of seven (7) days after written notice thereof by the GSMA to the defaulting party; and

(iii) upon 90 days written notice for any reason.

10.2 Upon the expiration or termination of the eSA or any participation thereof for any reason, each affected CB, or any Licensing Laboratories or EUMs will promptly return all copies of the GSMA's Confidential Information in its possession, power custody or control

10.3 The parties agree that except as otherwise provided herein, any obligations and duties either expressly or by their nature extend beyond the expiration or termination of this eSA, including, without limitation, Clauses 5, 6, 7 and 8.2 and Annex A shall survive the expiration or termination of this eSA.

11 FEES

11.1 All eSA Participants are under the obligation to pays the eSA License Fees set out in Annex A, during the eSA submission phase and before the evaluation by the licensed laboratory commence, directly to the GSMA.

12 GENERAL

12.1 Amendments to or modifications of the eSA STC may be made only by the GSMA.

12.2 A waiver by the GSMA of any breach by any other party of any terms, provisions or conditions of the eSA or the acquiescence of the GSMA and any act (whether by commission or omission) which but for such acquiescence would be a breach as aforesaid shall not constitute a general waiver of such term, provision or condition or of any subsequent act contrary thereto.

12.3 Any benefit of the eSA may not be assigned by a eSA Participant in whole or in part without the prior written consent of the GSMA.

12.4 This eSA represents the entire understanding of the GSMA concerning the subject matter hereof and overrides and supersedes all prior promises, representations, negotiations, undertakings, understandings, arrangements, agreements, side letters or heads of agreement concerning the same which are hereby revoked.

12.5 The GSMA shall not be responsible or liable for any failure or delay or consequence thereof in the performance of any of its obligations in this eSA owing to fire, strike, lock-out, lock-down, epidemic, industrial dispute, delay in transport, shortage of fuel, inability to obtain materials, embargo, act, refusal of licence, demand or requirement of any government or any government department or agency or of any local authority or of a consequence of war or of hostilities or armed conflict (whether war be declared or not) or to any other cause whatsoever beyond the GSMA's reasonable control or the after-effects of any of the foregoing and whether same take place or have effect in the United Kingdom or elsewhere.

12.6 Wherever provision is made in this eSA for the giving of any notice or communication to the GSMA, such notice or communication shall be in writing and shall be deemed to have been duly provided if sent by courier addressed to the GSMA entitled to receive the same or personally delivered to the GSMA, or sent by email transmission, in each case to the attention of the individual acting on behalf of such party specified below:

Title
GSM Association
1 Angel Ln,
London EC4R 3AB,
United Kingdom
Email: eSA@gsma.com

Any Notice in relation to the eSA shall be deemed to have been given on the day that it is so delivered personally or sent by successful email transmission or, if sent by courier, shall be deemed to have been given immediately upon delivery by the courier company.

12.7 Severability. If any provision of the eSA is agreed by the parties to be illegal, void or unenforceable under any law that is applicable hereto or if any court or arbitrator of competent jurisdiction in a final decision so determines, the eSA shall continue in force save that such provision shall be deemed to be deleted here from with effect from the date of such agreement or as declared by a decision of the said court or arbitrator or such earlier date as the GSMA may agree.

12.8 The eSA and the rights and obligations of the parties associated with it are governed by and construed in accordance with and subject to the laws of England and Wales, without reference to conflicts of laws principles. The parties hereby irrevocably submit to the exclusive jurisdiction of the Courts of England and Wales. In respect of the interpretation and enforcement of the provisions of the eSA, all documents referred to in this eSA and in

respect of the transactions contemplated hereby and the parties hereby waive the right to and agree not to assert that such applicable Court does not have exclusive jurisdiction.

Annex A - eSA License and Admin Fees

Introduction

Certification Bodies, EUMs and Licensed Laboratories interested in obtaining GSMA eSA certification need to budget for the costs associated with the eSA license and administration certification fees. This annex describes typical eSA license and administration certification costs that Certification Bodies, EUM and Licensed Laboratory should consider. The cost of the license and administration certification process will vary depending on the certification scope, the certification type, and whether the company is a GSMA member or not. All eSA fees are payable in Pounds (£). eSA certification fees must be paid in full and prior to the submission phase.

Certifications Types

- New Certification - This procedure shall be used for new product evaluations.
- Maintenance with Minor Changes - This procedure shall be used for changes of the TOE without security impact. Maintenance may not require involving a Licensed Laboratory. If it is not clear whether a security function has changed, the Developer shall assist the Certifier by providing an analysis from a Licensed Laboratory. The maintained certificate will have the same validity as the original certificate.
- Maintenance with Major Changes - This procedure shall be used for security relevant changes, where only the changed functionality will be assessed. It always requires the involvement of a Licensed Laboratory and the vulnerability analysis and testing are limited to the changes. The certificate validity from the original certificate will be kept.
- Re-Certification - This procedure shall be used to extend the certificate validity with or without changing the TOE. If major changes are present, then the evaluation focusses on the changes of the TOE using the current state-of-the-art attack techniques. If the TOE is not changed, then the vulnerability analysis and testing is updated considering the current state-of-the-art attack techniques.

Certifications Costs

A eSA Certification Body, eSA Licensed Laboratory and EUM must first provide the GSMA with a signed and dated copy of the eSA registration form by two duly authorized signatories set out in Annex B ("Registration") including the payment of their License and Administration Fee set out in this Annex ("eSA Fees") in full.

After the above step is completed an eSA Licensed Laboratory and EUM must then sent properly completed and signed application form and a draft Security Target (ST) for the eUICC product for certification to the GSMA CB that must have also sent back a quotation for certification for acceptance by the EUM before commencing the evaluation phase.

The Certification Administration fees and the Scheme Annual License Fees for the different certification types are as indicated in the following tables:

GSMA Certification Administration Fees

Certification Type	EUM
New Certification	£1,500
Maintenance with minor changes	£750
Maintenance with major changes	£1,000
Re-certification	£1,500

Certification Administration Fees are applicable per certification transaction

GSMA

eSIM

GSMA Certification Scheme Annual License Fees

Fee Type	Certification Body	Licensed Laboratory	EUM
Annual License Fee	£10,673 per annum	£13,342 per annum	£10,673 per annum

Special Conditions

- In the event that a Test Laboratories or EUM is an associate member of GSMA the Annual License Fee is discounted by 100%.
- In the event that an EUM is an associate member of the GSMA the Certification Administration Fee is discounted by 33.3%.
- In the event that an EUM is an associate member and an early eSA scheme adopters between Q4 2020 and Q1 2021 the GSMA the Certification Administration Fee is discounted by 100%.

General Terms

GSMA reserves the right to make adjustments to fees and discounts 1 April each calendar year.

Annex B - eSA Registration Form

For convenience this document is provided separately.

First Signatory		**Second Signatory**	
Signature		Signature	
Name		Name	
Position/Title		Position/Title	
Date		Date	