M2M IOT Trust Model
Version 1.0
30 November 2017

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Scope

This document is being undertaken to assess the effectiveness of the security of the business relationships between the different parties in the GSMA *Remote Provisioning Architecture for Embedded UICC*, [1] and [2].

1.2 Document Purpose

The aim of this document is to ensure that the dependencies between the different parties in the GSMA *Remote Provisioning Architecture for Embedded UICC*, [1] and [2] trust model is clear.

1.3 Intended Audience

The intended audience of this document is stakeholders with any interest in the trust model.

1.4 Definition of terms

Term	Description
Actor	An Actor is a physical entity (person, company or organisation) that can assume a Role in the functional architecture. It is possible for an Actor to assume multiple Roles in the same functional architecture.
Asset	Assets may be of different types, such as information, processes and systems. Within SM-DP and SM-SR the processes, information Assets and SM-DP or SM-SR, system Assets must be controlled and closely supervised so that they are secure.
Certificate Issuer	The Certificate Issuer (CI) Role issues the certificates for the eUICC remote provisioning system and acts as a trusted third party for the purpose of mutual authentication of the entities of the system
Mobile Network Operator (MNO)	A mobile network operator or mobile virtual network operator; a company providing wireless cellular network services.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC
Provisioning	The downloading and installation of a Profile into an eUICC
Role	Roles are representing a logical grouping of functions.
Subscription Manager Data Preparation	Role that prepares Operational and Provisioning Profiles to be securely provisioned on the eUICC and manages the installation of the Profile on the eUICC
Subscription Manager Secure Routing	Role that securely performs functions which allow secure transport of both Platform and Profile management commands in order to load, enable, disable and delete Profiles on the eUICC.

1.5 Abbreviations

Abbreviation	Description
CI	Certificate Issuer
ECASD	eUICC Controlling Authority Security Domain
eUICC	Embedded UICC
EUM	eUICC Manufacturer
GSMA	GSM Association
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
MNO	Mobile Network Operator
SAS	Security Accreditation Scheme
SAS-SM	Security Accreditation Scheme - Subscription Manager
SAS-UP	Security Accreditation Scheme – UICC Production
SM-DP	Subscription Manager - Data Preparation
SM-SR	Subscription Manager - Secure Routing

1.6 References

Ref	Document Number	Title
[1]	GSMA PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[2]	GSMA PRD SGP.02	Remote Provisioning Architecture for Embedded UICC – Technical Specification
[3]	GSMA PRD SGP.05	Embedded UICC Protection Profile
[4]	GSMA PRD SGP.11	Remote Provisioning Architecture for Embedded UICC – Test Specification
[5]	GSMA PRD SGP.14	GSMA eUICC PKI Certificate Policy
[6]	ETSI TS 102 225	Smart Cards; Secured packet structure for UICC based applications
[7]	ETSI TS 102 226	Smart Cards; Remote APDU structure for UICC based applications
[8]	GSMA PRD FS.04	SAS-UP Standard
[9]	GSMA PRD FS.05	SAS-UP Methodology
[10]	GSMA PRD FS.08	SAS-SM Standard
[11]	GSMA PRD FS.09	SAS-SM Methodology
[12]	GSMA PRD FS.17	Consolidated Security Requirements
[13]	GP Compliance Test Suite	GlobalPlatform eUICC Test Spec (v3.1) Compliance Test Suite v2.0.0.2
[14]	GP Amendment D	GlobalPlatform Card Specification Amendment D

2 Ecosystem

The following schema, extracted from the GSMA PRDs SGP.01 [1] and SGP.02 [2], specifies the Roles and communication interfaces associated with the remote provisioning and management of the Embedded UICC (eUICC), building on the GSMA PRD Remote Provisioning Architecture for Embedded UICC [1] [2].

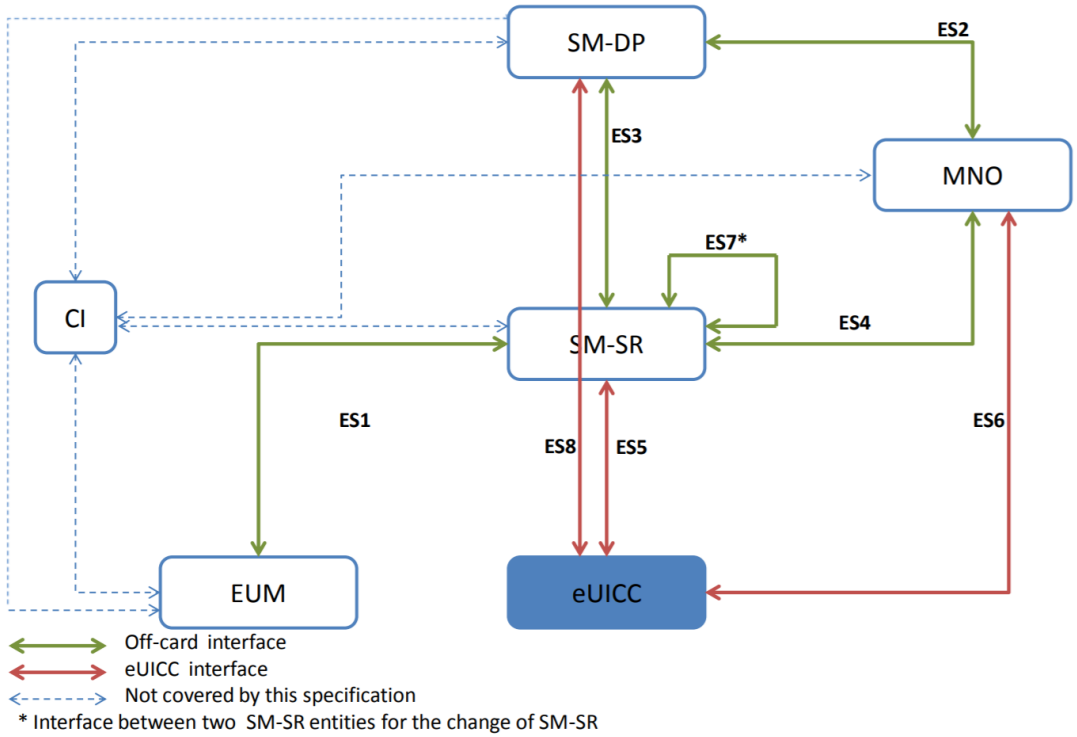

Figure 1: eUICC Remote Provisioning Architecture for M2M (SGP.01 and SGP.02)

Note: The existing communication interfaces which are incorporated by reference into the architecture will, in general, be assumed adequately secure and will not be covered in detail in this document.

3 Trust Definition

Trust is defined in this document to mean the following: A trusts B if *A believes B will enforce a security policy compatible with A's security policy for the Assets under consideration*. As an example: A trusts B to keep the same secrets as A and under equivalent security measures.

Note: This definition allows limitations on the scope of trust, as well as having the important property of *not* being transitive: 'A trusts B' and 'B trusts C' does *not* imply 'A trusts C'.

The above definition makes it possible to analyse a trust relationship in terms of assets governed by security policies: how far does the trust relation extend? What can lead to breaches etc.?

Similarly the usual definition of 'risk' as "probability of the event multiplied by the impact of the event" – i.e. a probable event with very low impact is a low risk, whereas a low probability event with a (very) high impact is a high risk.

In addition, in GSMA PRD SGP.01 [1] a concept of 'security realm' is used. This corresponds to the enforcement of one security policy across one single protected domain and operated by one single Actor. The establishment of trust between security realms is based on the ability of authentication and authorization between the realms and the check of the relevant security policies of each realm.

4 Trust Model

For the security of any system to be properly assessed and adequately addressed, non-technical aspects need to be considered as security cannot be achieved by technical means alone. Defining a trust model helps identify which Actors participate, what Roles they perform and which, and to what degree, they are to be trusted. Such an approach is designed to ensure serious security risks that may be posed by trusted insiders, as well as hostile outsiders, are identified and addressed. The trust model for the Remote Provisioning Architecture for Embedded UICC must ensure the probability of malicious Actors being able to access and negatively impact the system is minimised and that the level of risk posed by malicious insiders and outsiders is reduced.

This trust model describes the essentials of who the various stakeholders are in the remote provisioning ecosystem, what Role each stakeholder plays and what trust relationships exist between those stakeholders. Essentially, the trust model describes who trusts whom to do what and as decisions to trust are equivalent to accepting risks the model can be used to define necessary security requirements and policies, and where and to whom they should apply, to reduce risk.

The trust model for this architecture derives from the existing trust model for removable UICCs. The parties in that model are the Mobile Network Operator (MNO) and the UICC manufacturer.

The trust model for embedded UICC can be assumed to be the same as far as the relationships between those two parties go, but with the addition of three Roles: the Certificate Issuer, Subscription Manager - Data Preparation (SM-DP) and the Subscription Manager - Secure Routing (SM-SR).

5 Trust Model Roles

Roles represent a logical grouping of functions in a collection of functions that cannot be split up.

It is assumed that all Actors utilising products and services based on these specs will require the level of certification and compliance which is described in the specification. These assumptions are essential for the remote provisioning ecosystem to work as intended and

any breach of these must be considered as a flawed implementation of the system for remote provisioning. That is, the participation of un-certified or non-compliant Entities will result in an increased security risk.

5.1 Mobile Network Operator (MNO)

The architecture and technical solutions described in GSMA PRD SGP.01 [1] and GSMA PRD SGP.02 [2] assume that a MNO behaves according to the laws and regulations designed to deliver trust in whichever jurisdiction it operates. The MNO must not intentionally or knowingly engage in activities or behaviours that have the potential to undermine the trust placed in it by other stakeholders that have the potential to result in compromised security levels.

In terms of trust, all MNOs in the remote provisioning ecosystem trust each other to appropriately *manage the sensitive Assets.* Each MNO assumes that each other MNO enforces a security policy for Profile management and related sensitive Assets equivalent to its own.

The MNO or its delegated SM-DP ensures that Profile management commands delivered by the SM-SR are appropriate.

5.2 eUICC Manufacturer (EUM)

The eUICC Manufacturer (EUM) is responsible for producing the eUICC which is a central trusted component in the ecosystem. All ecosystem Actors trust the eUICC to protect sensitive Assets of the remote provisioning ecosystem.

This trust is anchored in the certification of the Security Accreditation Scheme – UICC Production EUM (GSMA SAS-UP [8] and [9]) and the certification of the eUICC itself (done against the eUICC Protection Profile SGP.05 [3]).

In addition, the eUICC communicates only with GSMA Security Accreditation Scheme - Subscription Manager (SAS-SM [10] and [11]) certified SM-DP and SM-SR. A GSMA SAS-SM certified SM-DP and/or SM-SR has a public key certificate signed by a Certificate Issuer, allowing it to be trusted by ecosystem Actors.

5.3 Subscription Manager Data Preparation (SM-DP)

The SM-DP acts on the instructions of the MNO. They can therefore be considered acting with delegated authority from the MNO: the MNO trusts the SM-DP with the delegated authority to manage their Profile information until downloaded and installed on the eUICC. Note that this trust covers all operations and procedures within the SM-DP handling Profile Assets in a secure manner. This assurance is provided through SAS certification of the SM-DP (http://gsma.com/sas).

The SM-DP may or may not have a relationship with the embedded UICC manufacturer.

5.4 Subscription Manager Secure Routing (SM-SR)

The MNO selects which SM-SR is allowed to manage its Profiles. Authority is given to the SM-SR by the EUM to manage the content of the eUICC to do the Provisioning. The SM-SR is configured by the EUM during the manufacturing process of the eUICC. After an MNO's Profile is downloaded to the eUICC, the SM-SR will act on this Profile on instructions from

that MNO (or the SM-DP on the MNO's behalf) independently of the EUM, so the SM-SR may be considered acting with delegated authority from the MNO.

It is possible to change the SM-SR during the eUICC lifecycle. Such a change is controlled by the MNO subject to business agreements. In that case, the new SM-SR will assume the responsibilities from the previous SM-SR. Only one SM-SR is associated to the eUICC at any time.

5.5 Certificate Issuer (CI)

The Certificate Issuer (CI) issues digital certificates to the EUMs, SM-DPs and SM-SRs and acts as a trusted third party for the purpose of mutual authentication of the eUICCs, SM-DPs and SM-SRs of the ecosystem.

6 Relationships and Dependencies

Figure 1 shows, in the form of data-flow diagrams, the relationships specified in the architecture and technical specification GSMA PRD SGP.01 [1] and GSMA PRD SGP.02 [2].

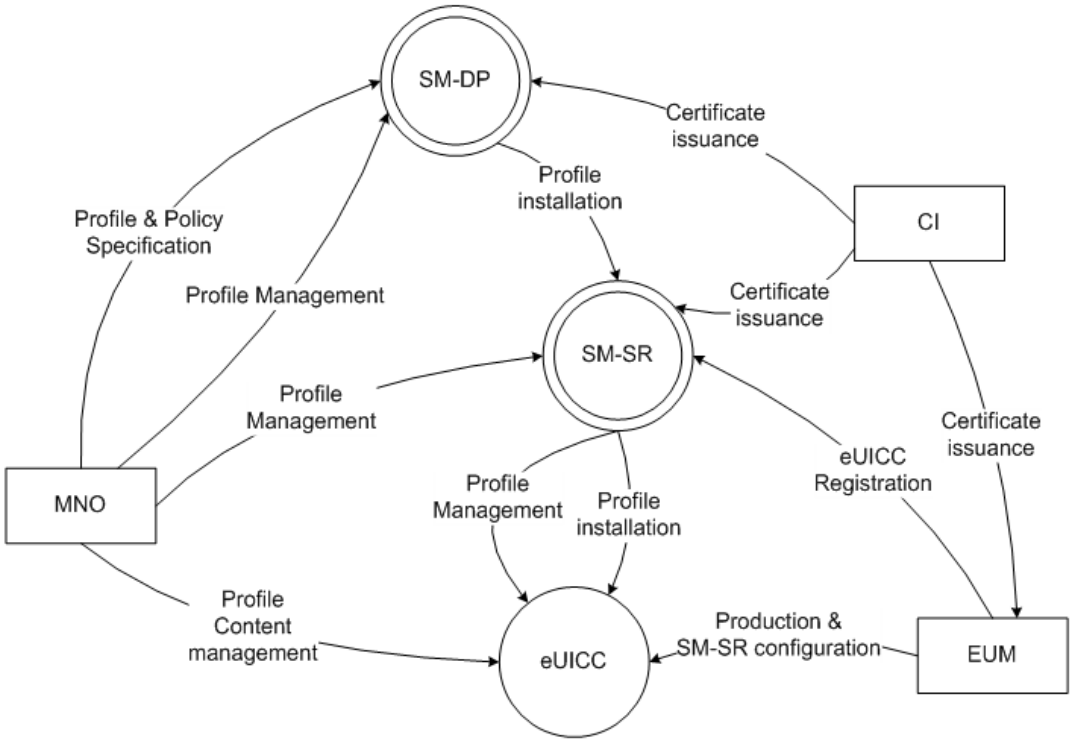

Figure 2: Data Flow

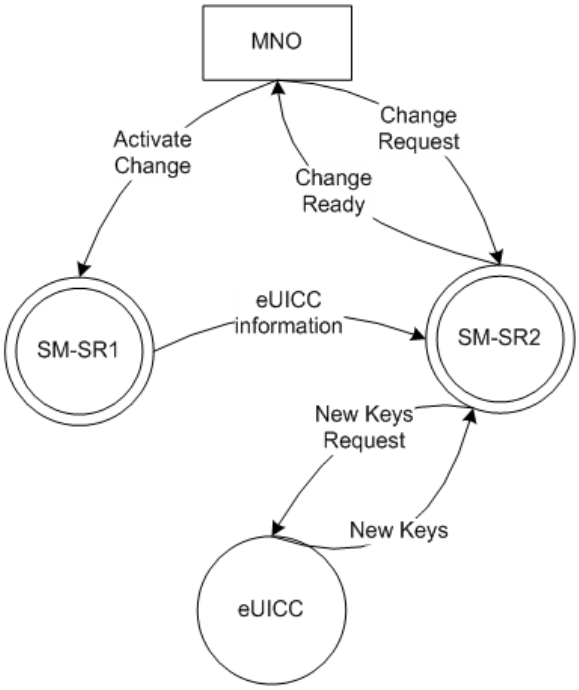

Figure 3: SM-SR Change Data Flow

6.1 Between MNO and SM-SR

The technical specification specifies that the communication interfaces between the MNO and the SM-SR may be based upon the processes and security requirements mutually defined and agreed. The security mechanisms for this interface are therefore not defined in the technical specification to allow the parties the freedom to use mechanisms of their choice and in accordance with local regulations.

6.2 Between MNO and SM-DP

The Technical Specification specifies that the communication interfaces between the MNO and the SM-DP may be based upon the processes and security requirements mutually defined and agreed. The security mechanisms for this interface are therefore not defined in the technical specification to allow the parties the freedom to use mechanisms of their choice and in accordance with local regulations.

6.3 Between MNO and eUICC

The communication interface between the MNO and the eUICC is used exclusively for Profile content management which uses the security mechanisms defined in ETSI TS 102 225 [6] and ETSI TS 102 226 [7].

6.4 Between SM-DP and SM-SR

The SM-SR and the SM-DP are both assumed to be SAS-SM certified (GSMA PRD SAS-SM [10] and [11]) and hence trusted by the MNO. In addition, the MNO can choose SM-DP

and SM-SR independently and both act on behalf of the MNO. The trust relation between SM-DP and SM-SR is established through mutual authentication which is performed prior to any management operation involving the SM-DP (as described in section 3.5 of GSMA PRD SGP.01[1]). This mutual authentication is only possible between certified SM-DPs and SM-SRs.

6.5 Between eUICC and SM-SR

The SM-SR is selected by the MNO and associated to the eUICC by the EUM during the manufacturing process. After the issuance of the eUICC by the EUM, if there is an SM-SR change during the lifecycle of the eUICC, this will be directly managed through the eUICC and current SM-SR.

6.6 Between eUICC and SM-DP

The SM-DP acts on behalf of the MNO and establishes a secure and authenticated channel to the eUICC to download and install Profiles on to the eUICC according to GlobalPlatform Card Specification Amendment D [14], as well as the variant SCP03t defined in GSMA PRD SGP.02 [2].

6.7 Between the Certificate Issuer and the EUM, SM-SR and SM-DP

The Certificate Issuer (CI) issues digital certificates to the EUMs, SM-DPs and SM-SRs.

7 Trust Enablers

The existing enablers available to the different parties to prevent malicious attacks are:

7.1 Certification

The certification comprises of three elements for the eUICC:

1. the production environment (GSMA PRD SAS-UP [8] and [9]),
2. the functional compliance (GSMA PRD SGP.11 [5] and GlobalPlatform eUICC Test Spec Compliance Test Suite [13] Compliance Program for eUICC)
3. the conformance to the Protection Profile (GSMA PRD SGP.05 [3])

The certification comprises of two elements for the SM-SR and SM-DP:

1. the Subscription Management operational site security (GSMA PRD SAS-SM [10] and [11])
2. the functional compliance (GSMA PRD SGP.11 [5] using own methods)

SAS-SM certified SM-DPs and SM-SRs will have digital certificates from the Certificate Issuer to prove such certification.

The SAS-UP certified EUM with a digital certificate from the Certificate Issuer will be able to provide eUICC products that have successfully achieved the functional compliance and the conformance to the Protection Profile as stated above.

8 Trust Summary

In the remote provisioning ecosystem, the issue of restricting access is designed to be resolved by the certification and accreditation of the various Actors by qualified and neutral third parties, including auditors and accreditation bodies. This is entirely consistent with best practice which has been employed by many industries and sectors for a number of years. The certification and accreditation initiatives can be effective in reducing risks but only ensure that a malicious insider in the ecosystem is as secure as the others and hence they do not protect against all attacks.

The second issue of how to detect and stop malicious insiders is somewhat resolved by administrative mechanisms in the SM systems and the MNO back-office systems. However, security always requires some trade-offs and compromises to be made to ensure systems remain usable and efficient to run. Consequently, complex and cumbersome technical security controls are not always required, or likely to be effective, and some security issues are addressed by the GSMA SAS Certification scheme's non-technical security requirements (GSMA PRD FS.17[12]) and these include requirements on employee screening which are flagged but are not defined in the technical specification.

The security and reliability of the remote provisioning ecosystem is enabled by the correct implementation of a range of different security requirements, not just those that are purely technical in nature, and these are defined in the remote provisioning GSMA SAS certification and accreditation requirements.

A remote provisioning trust model is relatively simple with just a few well defined Roles and relationships. This is illustrated in the fact that the Issuer Security Domain Root (ISD-R), Issuer Security Domain Profile (ISD-P) and eUICC Controlling Authority Security Domain (ECASD) are all combined onto the eUICC. This means that the remote provisioning trust model consists of just five Roles which are physically separate: MNO, EUM, SM-DP SM-SR and Certificate Issuer. The small number of just six dependencies reduces the attack surface and the opportunities for malicious insiders and outsiders with the result that the remote provisioning ecosystem is less prone to attack than other systems that manage similar Assets.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	30 Nov 17	First Version of M2M IOT Trust Model	SIM Group	Gloria Trujillo, GSMA

Other Information

Type	Description
Document Owner	Gloria Trujillo
Editor / Company	GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.