

eUICC Profile Package: Interoperable Format Technical Specification

Early Deployment of Version 2.3 for 5G Support

Published by  **simalliance** now Trusted Connectivity Alliance

October 2019

Copyright © 2019 Trusted Connectivity Alliance Ltd.

The information contained in this document may be used, disclosed and reproduced without the prior written authorization of Trusted Connectivity Alliance. Readers are advised that Trusted Connectivity Alliance reserves the right to amend and update this document without prior notice. Updated versions will be published on the Trusted Connectivity Alliance website at

<http://www.trustedconnectivityalliance.org>

Intellectual Property Rights (IPR) Disclaimer

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance's website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below.

Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.

Table of Contents

1. Objective.....	4
2. Issues to be solved.....	4
3. Recommendations.....	4

1. Objective

The objective of this document is to guide the implementers of V2.3 of the Profile Package technical specification in case it is used in an eUICC developed according to V2.2.1 or earlier of the GSMA specification SGP.22 (RSP technical specification).

2. Issues to be solved

As mentioned in Annex F of the Profile Package technical specification V2.3, installing a Profile containing support for 5G SUCI calculation by the USIM on an eUICC supporting only V2.2 or earlier of this specification may cause some trouble to the terminal.

"5G support:

In case a V2.3 profile requesting SUCI calculation (i.e. DF 5GS and/or DF SAIP and service n°124 and/or service n°125 are available in the EF_UST) would be downloaded on an eUICC that does not support SUCI calculation and this eUICC is soldered or inserted in a 5G ME, the service indicators related to SUCI calculation in the UST would be ignored by the eUICC but they would be understood by the 5G ME. The 5G ME may send a GET IDENTITY command or try to read the content of DF 5GS. The GET IDENTITY command would then fail because the eUICC OS does not support SUCI calculation by USIM or the terminal would not find the information required for the SUCI calculation."

In order to avoid this issue, V2.3 of the specification mandates that when the 2 new PEs are used in order to support 5G SUCI calculation then they shall be flagged as "Mandated".

In GSMA specification SGP.22 V2.2.1 and earlier, there are some exchange of information between the SM-DP+ and the eUICC in order to check the compliance of the eUICC with the features required by the Profile intended to be downloaded. During this eligibility check, the eUICC shall send the version of the Profile Package specification as well as a list of optional features which are supported.

The support of version 2.3 of the Profile Package specification can be reported to the SM-DP+ in compliance with SGP.22, however, the reporting of the support of features related to 5G SUCI calculation is not available. This recommendation explains how to report these features to the SM-DP+.

3. Recommendations

An eUICC compliant with V2.3 of the SIMalliance Profile Package specification and compliant with V2.2.1 and earlier of GSMA SGP.22 RSP specification shall comply with the following additional recommendations:

1. The `profileVersion` filed in the `EUICCInfo2` data object shall report support of version 2.3.
2. If the eUICC supports 5G SUCI calculation by the USIM:

The coding of `UICCCapability` shall be modified in the following way:

```
-- Definition of UICCCapability
UICCCapability ::= BIT STRING {
-- Sequence is derived from ServicesList[] defined in SIMalliance PDefinitions
  contactlessSupport(0), -- Contactless (SWP, HCI and associated APIs)
  usimSupport(1),        -- USIM as defined by 3GPP
```

```

isimSupport(2),          -- ISIM as defined by 3GPP
csimSupport(3),         -- CSIM as defined by 3GPP2

akaMilenage(4),         -- Milenage as AKA algorithm
akaCave(5),             -- CAVE as authentication algorithm
akaTuak128(6),          -- TUAK as AKA algorithm with 128 bit key length
akaTuak256(7),          -- TUAK as AKA algorithm with 256 bit key length
usimTestAlgorithm(8),   -- USIM test algorithm
rfu2(9),                -- reserved for further algorithms

gbaAuthenUsim(10),      -- GBA authentication in the context of USIM
gbaAuthenISim(11),      -- GBA authentication in the context of ISIM
mbmsAuthenUsim(12),     -- MBMS authentication in the context of USIM
eapClient(13),          -- EAP client

javacard(14),           -- Java Card(TM) support
multos(15),             -- Multos support

multipleUsimSupport(16), -- Multiple USIM applications are supported within the
same Profile
multipleIsimSupport(17), -- Multiple ISIM applications are supported within the
same Profile
multipleCsimSupport(18), -- Multiple CSIM applications are supported within the same
Profile

berTlvFileSupport(19),  -- BER TLV files
dfLinkSupport(20),      -- Linked Directory Files
cat-tpSupport(21),      -- CAT_TP support by any SD with SCP80
get-identitySupport(22), -- Support of GET IDENTITY as defined in ETSI TS 102 221
and the associated interface for SUCI derivation as defined in 3GPP TS 31.130
profile-a-x25519Support(23), -- Support of ECIES Profile A as described in 3GPP TS
33.501
profile-b-p256Support(24) -- Support of ECIES Profile B as described in 3GPP TS
33.501
}

```