eSIM Application Note

Handling of SGP.29 EIDs in SGP.02 and SGP.22

29 October 2020

eSIM Application Note, 29 October 2020

## Handling of SGP.29 EIDs in the Context of SGP.02 and SGP.22

Overview

The purpose of this Application Note is to provide information about the use of EIDs issued in accordance with SGP.29, specifically, those whose first two digits are not '89', and how interoperability with existing servers can be ensured.

EID Formats

SGP.02 v3.2 and v4.x section 2.2.2 specifies the eUICC IDentifier (EID) as a 32-digit decimal value based upon ITU-T E.118. The EID begins with the digits '89' followed by a three-digit country code and a three-digit issuer identifier; the remaining section dedicates 5 digits to platform and OS version information, and 17 free digits, then a pair of check digits. SGP.22 v2.2.2 defines the EID by reference to SGP.02.

SGP.29 defines the structure and assignment process for EIDs that begin with digits other than '89'. In particular, the EID comprises three fields: the EUM Identification Number (EIN), the EUM Specific Identification Number (ESIN), and the check digits:
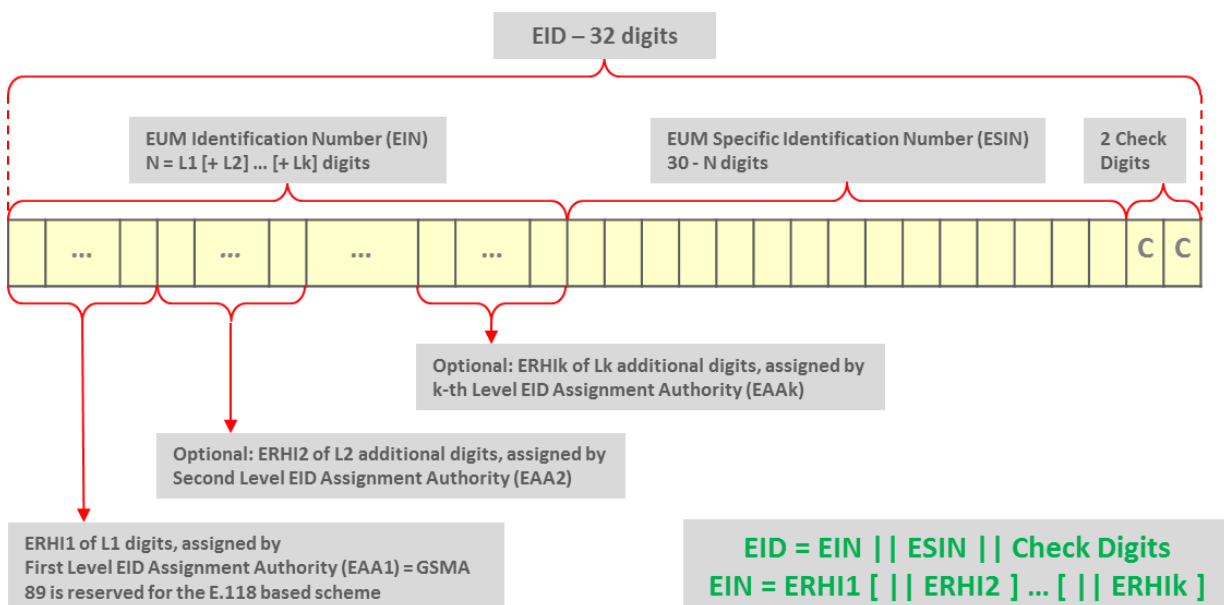
If EIDs following the general format permitted by SGP.29 are used in eUICCs, interoperability issues might result with servers that are compliant to existing specifications.

Consumer eSIM (SGP.22 v2.2.2)

SGP.22 defines the Issuer Identifier Number (IIN) as "The first 8 digits of the EID identifying the EUM issuing the eUICC," and refers to the IIN in multiple places. In particular, the serialNumber Name Constraint in the EUM certificate (section 4.5.2.1.0.2), and the Subject value in the eUICC certificate (section 4.5.2.1.0.3), explicitly refer to the IIN and state that it is the first 8 digits of the EID. An SM-DP+ or SM-DS compare the serialNumber Name Constraint in the EUM certificate against the 8-digit IIN of the EID in the eUICC certificate. This ensures that the EUM does not issue certificates for EID ranges it does not control. However, EIDs issued according to SGP.29 do not have an 8-digit IIN; instead, they have a variable-length EIN. This requires care by the EUM and the server providers to maintain interoperability between v2.2.2-compliant SM-DP+s and SM-DS and v2.2.2 eUICCs with SGP.29-compliant EIDs.

The serialNumber Name Constraint is a particular concern. If the EUM certificate were to specify a Name Constraint that was not 8 digits, this might be rejected by existing SM-DP+ and SM-DS servers. For that reason, it is strongly recommended that this Name Constraint always be 8 digits long. This results in the following cases:

- If the EIN is 8 digits long, then the Name Constraint exactly matches the EIN. Note that this will always be the case for a legacy EID (one that begins with '89').
- If the EIN is longer than 8 digits, then the Name Constraint does not fully specify the EIN. In this case the Name Constraint cannot fully ensure that EUMs assign values only within their ranges. This situation might arise in a setup with a National Authority – however, and at present, National Authorities are expected to continue using the legacy ('89') scheme.
- If the EIN is shorter than 8 digits, then the Name Constraint also includes the first few digits of the ESIN. This effectively reduces the number of digits available in the ESIN. The EUM will need to take care that these digits are assigned the same values in all EIDs.

M2M eSIM (SGP.02 v3.x, v4.x)

SGP.02 specifies the structure of the EID, including specific digits dedicated to version information.

- The implicit 8-digit prefix ('89' + country code + issuer identifier) is important to ensure uniqueness of the EID across all EUMs.
- However, the remaining digits are assigned according to EUM-specific allocation schemes.
- Nothing in the specifications leverages the structure: in all procedures and functions, the EID is an opaque, unique, identifier.

SGP.02 references indirectly SGP.22 v2.1 for the format of the EUM Certificate (including the serialNumber Name Constraint). However, the eUICC Certificates follow GlobalPlatform format, where there is no Distinguished Name value. Therefore, the Name Constraint is not enforced by X.509 mechanisms. However, it may be verified at application level.

Recommendations

Consumer eSIM (SGP.22 v2.2.2)

1. eSIM functional entities (eUICC, LPA, SM-DP+, SM-DS) should not assume any structure of the EID other than the format specified in SGP.29. In particular, they should not assume that the EID always begins with '89', nor that it contains an 8-digit IIN, nor expect any specific structure for the digits comprising the ESIN (as specified in SGP.02). They should continue to handle the check digits as previously specified.
2. The serialNumber Name Constraint should be the first 8 digits of the EID, regardless of the length of the EIN.
3. The SM-DP+ and SM-DS should compare the serialNumber Name Constraint against the first 8 digits of the EID, regardless of the EIN.
4. If the EIN is shorter than 8 digits, the EUM should not assign different values for the leading digits of the ESIN.

M2M eSIM (SGP.02 v3.x, v4.x)

1. eSIM functional entities (eUICC, SM-DP, SM-SR) should not assume any structure of the EID other than the format specified in SGP.29. In particular, they should not assume that the EID always begins with '89', nor that it contains an 8-digit IIN, nor expect any specific structure for the digits comprising the ESIN. They should continue to handle the check digits as previously specified.
2. The serialNumber Name Constraint should be the first 8 digits of the EID, regardless of the length of the EIN.
3. The SM-SR and SM-DP may compare the serialNumber Name Constraint against the first 8 digits of the EID, regardless of the EIN.
4. If the EIN is shorter than 8 digits, the EUM should not assign different values for the leading digits of the ESIN