|  |  |
| --- | --- |
| 3GPP TR 31.826 V18.0.0 (2023-03) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  Study on new UICC application for NSSAA  (Release 18) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Abbreviations 8

4 Solutions overview 8

4.1 Introduction 8

4.2 Key issues 8

4.2.1 Multiple NSSAA contexts 8

4.2.2 Discovery of the supported features 8

4.2.3 EAP framework 9

4.3 Solution 1 9

4.3.1 Multiple NSSAA contexts 9

4.3.2 Discovery of the supported features 9

4.3.2.1 EAP Identifier 10

4.3.2.1.1 EFEAP-ID (EAP Identifier) 10

4.3.2.2 S-NSSAI list 10

4.3.2.2.1 EFS-NSSAI (S-NSSAI list) 10

4.3.2.3 EAP authentication status 11

4.3.2.3.1 EFEAP-STATUS (EAP Authentication STATUS) 11

4.3.3 EAP framework 12

4.3.3.1 NSSAA application management procedures 12

4.3.3.1.1 NSSAA application selection 12

4.3.3.1.2 NSSAA application initialisation 12

4.3.3.1.3 NSSAA application termination 12

4.3.3.1.4 NSSAA application closure 13

4.3.4 Security features 13

4.3.4.1 User verification and file access conditions 13

4.3.5 NSSAA application commands 13

4.3.5.1 AUTHENTICATE 13

4.3.5.1.1 Command description 13

4.3.5.1.1.1 Command parameters and data 14

4.3.5.1.1.2 Specific status conditions returned 15

4.3.5.1.1.3 Status words 15

4.3.6 List of SFI values (annex) 15

5 Evaluation criteria 15

5.1 Overview 15

5.2 Key issues addressed 15

5.3 Impact on USIM and ISIM 15

5.4 Impact on UICC 15

5.5 Backward compatibility 16

5.6 Impact on core and RAN networks 16

6 Solutions evaluations 16

6.1 Solution 1 16

6.1.1 Key issues 16

6.1.2 USIM and ISIM types applicable 16

6.1.3 Impact on UICC 16

6.1.4 Backward compatibility 16

6.1.5 Impact on core and RAN networks 16

7 Conclusion 16

Annex A (informative): Change history 17

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

SA3 has finalized their security requirements on network slice-specific authentication and authorization (NSSAA) in 3GPP TS 33.501 clause 16 introduced in Release 16.

Among these requirements, there are few with potential UICC impact and hence need CT6's attention.

# 1 Scope

The aim of this Technical Report is to study the aspects for any potential enhancements on the UICC to be developed by CT6 based on the outcome of 3GPP TS 33.501. This work does not include selecting or standardizing any specific EAP method or associated EAP credential types for NSSAA.

For each of the objectives in the scope of the CT6 study, the UICC aspects that are to be covered in this study are as follows:

- Enhancements to support network slice-specific authentication and authorization using the UICC

- Study potential solutions for slice-specific authentication using new specific UICC application

- Study information the UICC application for NSSAA needs to contain

- Study information needed by the ME to select the correct UICC application used for NSSAA, in the case where multiple such UICC applications are available on the UICC. This information will not include UICC application selection based on a specific EAP method or type of EAP credentials.

- Study the interface that the new UICC application should feature in order to support NSSAA

Note: The study item in CT6 will not cover any security-related aspects within SA3's remit.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] ETSI TS 102 310: "Extensible Authentication Protocol support in the UICC".

[5] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[6] ISO/IEC 8825-1 (2008): "Information technology – ASN.1 encoding rules : Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[7] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[8] 3GPP TS 33.501: "Security Architecture and procedures for 5G system".

[9] ISO/IEC 7816‑4: "Identification cards - Integrated circuit cards,Part 4: Organization, security and commands for interchange".

[10] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[11] IETF RFC 2716: "PPP EAP TLS Authentication Protocol".

[12] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

**authenticator:** end of the EAP link initiating EAP authentication

**peer or supplicant:** end of the EAP Link that responds to the authenticator

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AAA-S Authentication, Authorization and Accounting Server

EAP Extensible Authentication Protocol

NSSAA Network Slice-Specific Authentication and Authorization

S-NSSAI Single Network Slice Selection Assistance Information

# 4 Solutions overview

## 4.1 Introduction

As defined in TS 24.501 [2] since Release 17, the purpose of the network slice-specific authentication and authorization (NSSAA) procedure is to enable the authentication, authorization and accounting server (AAA‑S) via the Network Slice Specific and SNPN Authentication and Authorization Function (NSSAAF) to (re‑)authenticate or (re‑)authorize the upper layers of the UE.

The NSSAA procedure can be invoked for a UE supporting it and for a HPLMN S-NSSAI or an SNPN S-NSSAI.

The NSSAA procedure is defined in TS 23.502 [3] clause 4.2.9 following the flow described in TS 23.502 [3] figure 4.2.9.2.1.

The NSSAA procedure is using the EAP framework. The end-points of the procedure are UE (supplicant) and AAA‑S (Authentication server) with AMF/SEAF in the middle (Authenticator). As described in TS 23.502 [3], the EAP ID and S-NSSAI are elements used by those end-points along the NSSAA procedure.

## 4.2 Key issues

### 4.2.1 Multiple NSSAA contexts

Multiple slices can be associated to different AAA‑S, belonging to different 3rd parties, and they can be active simultaneously. Consequently the UICC should be able to support at the same time multiple contexts for NSSAA.

### 4.2.2 Discovery of the supported features

The UICC may contain multiple applications (e.g. USIM, ISIM, IOPS). The ME should be able to check whether the UICC supports the NSSAA procedure, and in such case what is the appropriate application(s) to use from UICC to handle the NSSAA procedure.

### 4.2.3 EAP framework

The NSSAA is based on EAP procedure consisting in this document in:

- firstly to identify the supplicant counter-part of Authentication server in the UE

- secondly to transport the EAP messages between Authentication server and supplicant

The ME should be able to:

- retrieve from the UICC the elements (i.e. EAP ID and S-NSSAI) involved in the NSSAA procedure

- use the EAP framework implemented by the UICC to complete the NSSAA procedure

## 4.3 Solution 1

This solution uses most of the concept defined in ETSI TS 102 310 [4] which already specifies the EAP support in the UICC.

The EAP architecture is described in clause 5.1 from ETSI TS 102 310 [4].

However ETSI TS 102 310 [4] is not fully re-usable as is in the NSSAA context linked to the below points:

- EAP clients discovery as specified in clause 5.2 from ETSI TS 102 310 [4] is EAP method oriented when NSSAA service discovery should be independent of EAP method (S-NSSAI based)

- Elementary files as specified in clause 7 from ETSI TS 102 310 [4] are not needed in NSSAA context where only EAP Identifier and S-NSSAI information are necessary

The solution consist in:

- the UICC capable of supporting one or multiple NSSAA applications handling each a dedicated NSSAA context for each independent slice

- the NSSAA application discovery is based on the identification of supported S-NSSAI by a given NSSA application and retrieval of associated EAP identifier

- the NSSAA application is responsible for handling the EAP messages exchanged with EAP authentication server for a given NSSAA session via the ME

The following clauses detail how to address the key issues from clause 4.2.

### 4.3.1 Multiple NSSAA contexts

AAA‑S belongs to 3rd party and authentication to the AAA‑S is isolated from network access authentication.

In this solution, the isolation in the UICC between NSSAA authentication and USIM authentication is achieved with a new application: the ′NSSAA application′.

A NSSAA application supports the NSSAA procedure for a given list of S-NSSAI.

The NSSAA context enables the ME to associate a slice requiring a NSSAA with a given NSSAA application supporting the S-NSSAI of this slice.

The ME may access to more than one slice at the same time with different AAA‑S. This solution allows more than one NSSAA application(s) be active simultaneously in the UICC.

### 4.3.2 Discovery of the supported features

As defined in TS 31.101 [5], the ME reads the EFDIR to identify the appropriate application(s) to select and use.

This solution, similarly to '3GPP USIM (non-IMSI SUPI Type)' principle introduced in C6-xxxxx, defines a new 3GPP Application Code for 'NSSAA support' to identify the application(s) in the UICC supporting NSSAA procedure.

In case of more than one applications in EFDIR are available with 'NSSAA support' 3GPP Application Code, the ME retrieves the supported S-NSSAI list (see clause 4.3.1.1) from each NSSAA application in EFDIR and the ME can create a NSSAA context with corresponding NSSAA application.

For each NSSAA context, the ME retrieves the EAP Identifier (see clause 4.3.1.2) used in the corresponding NSSAA procedure.

NOTE: S-NSSAI lists from any NSSAA application are disjoint (do not contain common S-NSSAI).

#### 4.3.2.1 EAP Identifier

The EAP Identifier used during the NSSAA procedure is defined at NSSAA application level to be retrieved and used by the ME.

##### 4.3.2.1.1 EFEAP-ID (EAP Identifier)

This EF is available at application level of any NSSAA application.

This EF contains the EAP Identifier.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Identifier: '6F01' | | Structure: transparent | | | Mandatory | |
| SFI: '01' | | |  | | | |
| File size: X bytes | | | Update activity: low | | | |
| Access Conditions:  READ PIN  UPDATE ADM  DEACTIVATE ADM  ACTIVATE ADM | | | | | | |
| Bytes | Description | | | M/O | | Length |
| 1 to X | EAP ID TLV data object | | | M | | X bytes |

EAP ID

Contents:

- EAP ID for the slice authentication

Coding: the coding of EAP ID TLV data object is described hereafter.

|  |  |  |  |
| --- | --- | --- | --- |
| Length | Description | Value | Status |
| 1 byte | EAP ID Tag | 81 | M |
| 1 byte | Length (see note 1) | Z | M |
| Z bytes | EAP Identifier | -- | M |
| Note 1: coded according to ISO/IEC 8825-1 [6]. | | | |

#### 4.3.2.2 S-NSSAI list

The S-NSSAI list supported by any NSSAA application is defined at the NSSAA application level.

##### 4.3.2.2.1 EFS-NSSAI (S-NSSAI list)

This EF is available at application level of any NSSAA application.

This EF contains one or more records, each indicating the S-NSSAI supported by the NSSAA application.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Identifier: '6F02' | | Structure: linear fixed | | | Mandatory | |
| SFI: '02' | | |  | | | |
| Record length: X bytes | | | Update activity: low | | | |
| Access Conditions:  READ PIN  UPDATE ADM  DEACTIVATE ADM  ACTIVATE ADM | | | | | | |
| Bytes | Description | | | M/O | | Length |
| 1 to X | S-NSSAI | | | M | | X bytes |

S-NSSAI

Contents:

- S-NSSAI for which the NSSAA application is used for NSSAA procedure

Coding:

- S-NSSAI shall be coded as specified in TS 23.003 [7]

#### 4.3.2.3 EAP authentication status

The EAP authentication status is defined at NSSAA application level and can be retrieved by the ME.

##### 4.3.2.3.1 EFEAP-STATUS (EAP Authentication STATUS)

This EF contains the authentication status corresponding to the EAP client supported by the NSSAA application.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Identifier: '6F03' | | Structure: transparent | | | Mandatory | |
| SFI: '03' | | |  | | | |
| File size: 1 bytes | | | Update activity: low | | | |
| Access Conditions:  READ PIN  UPDATE ADM  DEACTIVATE ADM  ACTIVATE ADM | | | | | | |
| Bytes | Description | | | M/O | | Length |
| 1 | Authentication status | | | M | | 1 bytes |

Authentication Status

Contents:

- Status of the corresponding EAP authentication.

Coding:

- Authentication Status coded in one byte as below.

|  |  |
| --- | --- |
| Value | Meaning |
| '00' | No authentication started |
| '01' | Authenticating |
| '02' | Authenticated |
| '03' | Held (Authentication failure) |

### 4.3.3 EAP framework

This solution reuses the ETSI TS 102 310 [4] clause 6 specifying the EAP related commands to be supported by NSSAA application.

#### 4.3.3.1 NSSAA application management procedures

##### 4.3.3.1.1 NSSAA application selection

This solution proposes the perform NSSAA application selection in the following manner:

- When a slice procedure requires a NSSAA with a supported S-NSSAI from one of the NSSAA application defined in the UICC, the ME selects the corresponding NSSAA application using the SELECT by DF name as defined in TS 31.101 [5];

- This selection occurs after the UICC activation, defined in TS 31.101 [5], and the discovery of the NSSAA services described in above clause 4.3.2.

After a successful NSSAA application selection, the selected NSSAA application is stored on the UICC. This NSSAA application is identified as the 'last selected NSSAA application' by the UICC. The last selected NSSAA application is available on the UICC after a UICC deactivation followed by a UICC activation.

If a NSSAA application is selected using partial DF name, the partial DF name supplied in the command is uniquely identify a NSSAA application. Furthermore if a NSSAA application is selected using a partial DF name as specified in TS 31.101 [5] indicating in the SELECT command the last occurrence, the UICC selects the NSSAA application stored as the last selected NSSAA application. If, in the SELECT command, the options first, next/previous are indicated, they have no meaning if an NSSAA application has not been previously selected in the same session and shall return an appropriate error code.

When the NSSAA application is associated to an NSSAA context the application is kept selected.

##### 4.3.3.1.2 NSSAA application initialisation

##### 4.3.3.1.3 NSSAA application termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in TS 31.101 [5].

The ME terminates the NSSAA session with the NSSAA application as follows:

- The ME indicates to the NSSAA application by sending a particular STATUS command that the termination procedure is starting

The ME deletes all these subscriber related information elements from its memory

NOTE 2: If the ME has already updated any of the subscriber related information during the NSSAA session, and the value has not changed until NSSAA session termination, the ME may omit the respective update procedure.

To actually terminate the session, the ME shall then use one of the mechanisms described in TS 31.101 [5].

##### 4.3.3.1.4 NSSAA application closure

After termination of the NSSAA session as defined in previous clause, the NSSAA application may be closed by closing the logical channels that are used to communicate with this particular NSSAA application.

### 4.3.4 Security features

The security aspects of NSSAA are specified in TS 33.501 [8]. This clause gives information related to security features supported by the NSSAA application with respect to user verification and file access conditions.

#### 4.3.4.1 User verification and file access conditions

The security architecture as defined in TS 31.101 [5] applies to the NSSAA application and UICC with the following definitions and additions:

- The NSSAA application uses a global key reference as PIN1 as specified in TS 31.101 [5].

- The only valid usage qualifier is '08' which means user authentication knowledge based (PIN) as defined in ISO/IEC 7816-4 [9].

### 4.3.5 NSSAA application commands

The commands specified in TS 31.101 [5] are supported by NSSAA application, with the restrictions identified in this clause.

#### 4.3.5.1 AUTHENTICATE

The commands specified in TS 31.101 [5] are supported by NSSAA application, with the restrictions identified in this clause.

##### 4.3.5.1.1 Command description

The function is used to transfer the EAP packets from the ME to the selected NSSAA application (i.e. NSSAA that corresponds to the slice requiring NSSAA).

The NSSAA application provides a response EAP packet (as defined in RFC 3748 [10]) or a warning status word according to the authentication method being used.

The NSSAA application maintains the state machine of the authentication process as described for the particular EAP method used.

The function is related to a particular NSSAA application and can not be executable unless this NSSAA application has been selected and activated.

The format of the EAP packet is defined by the NSSAA application and respects the conventions corresponding for the EAP method.

The following EAP packets are allowed input packets for this command: EAP packets with code field equal to 1 "Request", 3 "Success" or 4 "Failure" and EAP packets with code equal to 2 "Response" for EAP type 1 "Identity" (Code and type values as defined in RFC 3748 [10]).

NOTE: EAP Identity is provided by the NSSAA application.

The command and response data may contain specific EAP method related data as an additional input/output parameter (e.g. gmt\_unix\_time for EAP-TLS implementations as defined in RFC 2716 [11]).

Depending on the length of the EAP input data, the EAP Authenticate may be used with an EVEN or ODD INS code. In the latter case, the EAP input and response data shall be encapsulated in BER TLV data objects, as specified in ETSI TS 102 221 [12].

Input:

- EAP Packet;

- EAP method related data.

Output:

- Either none (i.e. if authentication successful: EAP success packet received).

Or:

- EAP Response Packet;

- EAP method related data.

###### 4.3.5.1.1.1 Command parameters and data

|  |  |
| --- | --- |
| Code | Value |
| CLA | As specified in ETSI TS 102 221 [12] |
| INS | As specified in ETSI TS 102 221 [12] |
| P1 | As specified in ETSI TS 102 221 [12] |
| P2 | 00 |
| Lc | Length of subsequent EAP command data |
| Data | See below |
| Le | Length of the response data |

Command data:

|  |  |  |
| --- | --- | --- |
| Byte(s) | Description | Length |
| 1 to Lc | EAP command data (see table 4.3.5.1.1.1) | Lc |

Table 4.3.5.1.1.1: Coding of EAP command data

|  |  |  |  |
| --- | --- | --- | --- |
| Byte(s) | Description | Status | Length |
| 1 to J | EAP packet (coded as defined for the method of EAP used as defined in RFC 3748 [10]) | M | J bytes |
| J+1 to J+K+1 | EAP method related data (specified by each application specific document defining a particular EAP method implementation) | O | K bytes |
| NOTE: The length of an EAP packet is contained within the packet and can therefore be retrieved from it. | | | |

Response data:

|  |  |  |
| --- | --- | --- |
| Byte(s) | Description | Length |
| 1 to Le | EAP Packet Response Data (see table 4.3.5.1.1.2) | Le |

Table 4.3.5.1.1.2: Coding of EAP Response data

|  |  |  |  |
| --- | --- | --- | --- |
| Byte(s) | Description | Status | Length |
| 1 to L | EAP packet | M | L bytes |
| L+1 to L+N+1 | EAP method related data (specified by each application specific document defining a particular EAP method implementation) | O | N bytes |
| NOTE: The length of an EAP packet is contained within the packet and can therefore be retrieved from it. | | | |

###### 4.3.5.1.1.2 Specific status conditions returned

This clause specifies the coding of the specific status words SW1 and SW2.

###### 4.3.5.1.1.3 Status words

Table 4.3.5.1.1.3 shows the meaning of possible status conditions returned.

Table 4.3.5.1.1.3: Status byte coding

|  |  |  |
| --- | --- | --- |
| SW1 | SW2 | Description |
| '62' | '00' | - No information given, state of non-volatile memory unchanged (EAP Packet silently ignored) |
| '98' | '62' | - Authentication error (EAP Failure Packet received) |

### 4.3.6 List of SFI values (annex)

This annex lists SFI values assigned in the present document for files at the NSAAA application level.

|  |  |  |
| --- | --- | --- |
| File Identifier | SFI | Description |
| '6F01' | '01' | EAP Identity (EFEAP-ID) |
| '6F02' | '02' | List of S-NSSAI (EFS-NSSAI) |
| '6F03' | '03' | EAP Authentication STATUS (EFEAP-STATUS) |

All other SFI values are reserved for future use.

# 5 Evaluation criteria

## 5.1 Overview

In addition to the key issues described in the present document, the potential solutions also need to be evaluated against operational criteria when assessing their suitability. This clause details the evaluation criteria for the solutions.

## 5.2 Key issues addressed

Each solution clearly identifies the key issues addressed by the solution.

The evaluation assesses whether this key issue is met and any limitations on the way it is met (e.g. if the solution is only applicable to aspects of the key issue).

## 5.3 Impact on USIM and ISIM

The evaluation should clearly identify the types of USIM/ISIM that the solution works with, whether modification of existing USIMs/ISIMs is required and describe the impacts on USIM/ISIM.

## 5.4 Impact on UICC

The evaluation should clearly identify the UICC that the solution works with, whether modification of the existing UICC is required and describe the impacts on the UICC.

## 5.5 Backward compatibility

The evaluation should clearly identify that the solution is backward compatible.

## 5.6 Impact on core and RAN networks

The evaluation should clearly identify any changes required in the core network and/or RAN.

# 6 Solutions evaluations

## 6.1 Solution 1

### 6.1.1 Key issues

This solution addresses all key issues.

### 6.1.2 USIM and ISIM types applicable

The solution has no impact nor on the USIM neither on the ISIM.

### 6.1.3 Impact on UICC

This solution has minor impact on the UICC, only a new application code to be defined for the new UICC application for NSSAA.

### 6.1.4 Backward compatibility

This solution is backward compatible.

### 6.1.5 Impact on core and RAN networks

The solution has no impact on the core network or RAN.

# 7 Conclusion

Based on the solutions and evaluations in the present document, normative work in 3GPP CT WG6 should be based on Solution 1.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-08 | CT6#112-e | C6-220430 |  |  |  | Initial version of TR - Skeleton document | 0.1.0 |
| 2023-02 | CT6#114 | C6-230105 |  |  |  | Evaluation criteria, Solution 1 evaluation and conclusion | 0.2.0 |
| 2023-03 | CT#99 | CP-230112 |  |  |  | Presented for information and approval | 1.0.0 |
| 2023-03 | CT#99 |  |  |  |  | TR Approved | 18.0.0 |