**3GPP TSG-T (Terminals) Meeting #26**
**Athens, Greece**
**8 - 10 December 2004**

***TP-040257***

**Agenda Item:** 5.3.3
**Source:** T3
**Title:** CRs to TS 31.103
**Document for:** approval

---

This document contains the following change requests that are approved by 3GPP TSG T3 and forwarded to 3GPP TSG T#26 for approval:

| Doc-2nd-Level | Spec | CR | Rev | Phase | Subject | Cat | Version-Current | Version-New | Work item |
|---|---|---|---|---|---|---|---|---|---|
| T3-040833 | 31.103 | 019 | - | Rel-6 | Storage of the lifetime of the GBA_U bootstrapped keys | B | 6.5.0 | 6.6.0 | TEI6 |
| T3-040853 | 31.103 | 020 | - | Rel-5 | Correction of non specific references | F | 5.7.0 | 5.8.0 | TEI5 |
| T3-040854 | 31.103 | 021 | - | Rel-6 | Correction of non specific references | F | 6.5.0 | 6.6.0 | TEI6 |

**3GPP TSG-T3 Meeting #33**
**Sophia Antipolis, France, 16-19 November 2004,**

***Tdoc ⌘T3-040833***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **TS 31.103** **CR** **019** ⌘**rev** **-** ⌘ Current version: **6.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Storage of the lifetime of the GBA_U bootstrapped keys |
| ***Source:*** | ⌘ | T3 |
| ***Work item code:*** | ⌘ | TEI6 |
| ***Date:*** | ⌘ | 18/11/2004 |
| ***Category:*** | ⌘ | **B** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*
*Ph2 (GSM Phase 2)*
*R96 (Release 1996)*
*R97 (Release 1997)*
*R98 (Release 1998)*
*R99 (Release 1999)*
*Rel-4 (Release 4)*
*Rel-5 (Release 5)*
*Rel-6 (Release 6)*
*Rel-7 (Release 7)*

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | In the descriptions of the GBA_U bootstrapping procedures in TS 33.220, it is stated that '*the UE shall perform a bootstrapping authentication … when the lifetime of the key in UE has expired*'.<br><br>Besides it is stated that when the UE is powered down, or when the UICC is removed, there is no need to delete the bootstrapped keys from storage in the UICC.<br><br>Therefore, in some cases, it is necessary to store the key lifetime with the associated B-TID on the UICC for further use by the ME. |
| ***Summary of change:*** | ⌘ | Introduction of the bootstrapping key lifetime in $EF_{GBABP}$ |
| ***Consequences if not approved:*** | ⌘ | |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 4.2.9 | | | |
| ***Other specs affected:*** | ⌘ | **Y** | **N** | Other core specifications | ⌘ |
| | | [ ] | [ ] | Test specifications | |
| | | [ ] | [ ] | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

## 4.2.9 $EF_{GBABP}$ (GBA Bootstrapping parameters)

This EF contains the AKA Random challenge (RAND) and Bootstrapping Transaction Identifier (B-TID) associated with a GBA bootstrapping procedure. This file shall be present if the GBA service (service number 2) is allocated in $EF_{IST}$ (ISIM Service Table).

| Identifier: '6FD5' | Structure: transparent | Optional |
|---|---|---|
| File length: L+X + N +32 bytes | Update activity: low | |

Access Conditions:

| | |
|---|---|
| READ | PIN |
| UPDATE | PIN |
| DEACTIVATE | ADM |
| ACTIVATE | ADM |

| Bytes | Description | M/O | Length |
|---|---|---|---|
| 1 | Length of RAND (X) | M | 1 byte |
| 2 to (X +1) | RAND | M | X bytes |
| X+2 | Length of B-TID (L) | M | 1 byte |
| (X+32) to (X+21+L) | B-TID | M | L bytes |
| X+L+3 | Length of key lifetime | M | 1 byte |
| (X+L+4) to (X+L+N+3) | Key lifetime | M | N bytes |

- Length of RAND
  Contents: number of bytes, not including this length byte, of RAND field

- RAND
  Contents: Random challenge used in the GBA_U bootstrapping procedure.
  Coding: as defined in 33.103 [13]

- Length of B-TID
  Contents: number of bytes, not including this length byte, of B-TID field

- B-TID
  Content: Bootstrapping Transaction Identifier the GBA_U bootstrapped keys
  Coding: As defined in TS 33.220 [25]

- Length of key lifetime
  Contents: number of bytes, not including this length byte, of key lifetime field

- Key lifetime
  Content: Lifetime of the GBA_U bootstrapped keys
  Coding: As defined in TS 33.220 [25]

**3GPP TSG-T3 #33**
**Sophia Antipolis, France**
**16-19 November 2004**

*T3-040853*

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **31.103** **CR** **020** ⌘ **rev** **-** ⌘ Current version: **5.7.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Correction of non specific references |
| ***Source:*** | ⌘ | T3 |
| ***Work item code:*** | ⌘ | TEI5 |
| ***Date:*** | ⌘ | 19/11/2004 |
| ***Category:*** | ⌘ | **F** |
| ***Release:*** | ⌘ | Rel-5 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*
*Ph2* *(GSM Phase 2)*
*R96* *(Release 1996)*
*R97* *(Release 1997)*
*R98* *(Release 1998)*
*R99* *(Release 1999)*
*Rel-4* *(Release 4)*
*Rel-5* *(Release 5)*
*Rel-6* *(Release 6)*
*Rel-7* *(Release 7)*

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | The non specific references to ETSI SCP specifications has been updated to be specific |
| ***Summary of change:*** | ⌘ | Release 5 added to the referenced document |
| ***Consequences if not approved:*** | ⌘ | The non specific reference implies that a Rel-5 specification would reference the latest release which implies that features of the latest release of the referenced specification would apply. The specifcation would be considered as non frozen as long as any referenced specification is updated with a new release. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2 |

| | Y | N | | |
|---|---|---|---|---|
| ***Other specs affected:*** ⌘ | | N | Other core specifications | ⌘ |
| | | N | Test specifications | |
| | | N | O&M Specifications | |

***Other comments:*** ⌘

**How to create CRs using this form:**
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) 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 TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

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

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[8] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange

[8a] ISO 646 (1983): "Information processing - ISO 7-bits coded characters set for information interchange".

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".

[11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (Release 4)".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Release 5)".

[23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers ".

[24] IETF RFC 2486: "The Network Access Identifier"

**3GPP TSG-T3 #33**
**Sophia Antipolis, France**
**16-19 November 2004**

*T3-040854*

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **31.103** **CR** **021** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Correction of non specific references |
| ***Source:*** | ⌘ | T3 |
| ***Work item code:*** | ⌘ | TEI6 |
| ***Date:*** | ⌘ | 19/11/2004 |
| ***Category:*** | ⌘ | **F** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*
*Ph2* *(GSM Phase 2)*
*R96* *(Release 1996)*
*R97* *(Release 1997)*
*R98* *(Release 1998)*
*R99* *(Release 1999)*
*Rel-4* *(Release 4)*
*Rel-5* *(Release 5)*
*Rel-6* *(Release 6)*
*Rel-7* *(Release 7)*

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | The non specific references to ETSI SCP specifications has been updated to be specific |
| ***Summary of change:*** | ⌘ | Release 6 added to the referenced document |
| ***Consequences if not approved:*** | ⌘ | The non specific reference implies that a Rel-6 specification would reference the latest release which implies that features of the latest release of the referenced specification would apply. The specifcation would be considered as non frozen as long as any referenced specification is updated with a new release. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2 |

| ***Other specs affected:*** ⌘ | Y | N | | ⌘ |
|---|---|---|---|---|
| | | N | Other core specifications | |
| | | N | Test specifications | |
| | | N | O&M Specifications | |

***Other comments:*** ⌘

**How to create CRs using this form:**
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) 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 TS 21.111: "USIM and IC Card Requirements".

[2] 3GPP TS 31.102: "Characteristics of the USIM Application".

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

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 33.103: "3G Security; Integration Guidelines".

[6] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[7] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

[8] void

[9] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[10] ISO/IEC 7816-9 (2000): "Identification cards - Integrated circuit(s) cards with contacts - Part 9: Additional interindustry commands and security attributes".

[11] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

[12] 3GPP TS 25.101: "UE Radio Transmission and Reception (FDD)".

[13] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[14] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[15] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[16] IETF RFC 3261: "SIP: Session Initiation Protocol".

[17] 3GPP TS 23.038: "Alphabets and language-specific information".

[18] ISO 639 (1988): "Code for the representation of names of languages".

[19] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (Release 4)".

[20] ISO/IEC 8825(1990): "Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)" Second Edition.

[21] 3GPP TS 22.101: "Service aspects; Service principles".

[22] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Release 6)".

[23] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers

[24] IETF RFC 2486: "The Network Access Identifier"

[25] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture"

[26] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication". (http://www.ietf.org/rfc/rfc2617.txt)