

Agenda Item: 5.3.3
Source: T3
Title: CRs to TS 31.113
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	Workitem
T3-040845	31.113	027	-	Rel-5	Correction of reference to SCP specification	F	5.5.0	5.6.0	TEI5
T3-040846	31.113	028	-	Rel-6	Correction of reference to SCP specification	A	6.2.0	6.3.0	TEI5

CHANGE REQUEST

⌘ **31.113 CR 027** ⌘ rev **-** ⌘ Current version: **5.5.0** ⌘

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 ME Radio Access Network Core Network

Title:	⌘ Correction of reference to SCP specification		
Source:	⌘ T3		
Work item code:	⌘ TEI	Date:	⌘ 18/11/2004
Category:	⌘ F	Release:	⌘ Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)	Ph2 (GSM Phase 2)	
	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	
	B (addition of feature),	R97 (Release 1997)	
	C (functional modification of feature)	R98 (Release 1998)	
	D (editorial modification)	R99 (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)
			Rel-7 (Release 7)

Reason for change:	⌘ There was a discussion during TSG-T3 #32 on references to the SCP specifications, where if non-specific, it implies that later release features could be invoked into early release specifications by stealth (e.g. Rel-6 features into Rel-4 specifications by reference). To avoid this reference issue within the USAT Interpreter specifications, the reference to a SCP specification is replaced by a reference to the corresponding 3GPP specification.
Summary of change:	⌘ Reference to TS 102 221 is replaced by a reference to 3GPP TS 31.101.
Consequences if not approved:	⌘ Unclear usage of references.

Clauses affected:	⌘ 2, 6.1.1.1, 7.5						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<input checked="" type="checkbox"/>	Test specifications					
	<input checked="" type="checkbox"/>	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 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 TS 31.111: "USIM Application Toolkit (USAT)".

[2] 3GPP TS 31.114: "USAT Interpreter protocol and administration".

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

[4] [3GPP TS 31.101](#): "~~ETSI TS 102 221: "Smart cards; UICC-t~~ Terminal interface; Physical and logical characteristics".

[5] ISO/IEC 7816-6 (1995): "Identification cards – Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements".

[6] ISO 8731-1 (1987): "Banking – Approved algorithms for message authentication – Part 1: DEA".

[7] IETF RFC 1738: "Uniform Resource Locators (URL)"

[8] Schneier, Bruce: "Applied Cryptography Second Edition: Protocols, Algorithms and Source code in C", John Wiley & Sons, 1996, ISBN 0-471-12845-7.

[...]

6.1.1 Environment variable usage area

This usage area consists of 3 different partitions:

- USAT Interpreter system information partition;
- USIM issuer information partition;
- End user information partition.

6.1.1.1 USAT Interpreter system information partition

The USAT Interpreter partition is preloaded during the manufacturing process of the USIM or during the runtime of the USAT Interpreter.

At least the following information shall be stored:

Variable ID	Description	Coding
'00'	ICCID of UICC	Binary coding as for EF _{ICCID} specified in 3GPP TS 31.101 SCP TS 102-224 [4]
'01'	USAT Interpreter version	<p>Byte 1: Issuer Version USAT Interpreter issuer specific version. The coding and value of this byte depends on the USAT Interpreter issuer. The USAT Interpreter issuer is stored in variable '07' and variable '08'.</p> <p>Bytes 2-3: TS 31.113, Version (this TS) Byte 2: first digit (x according to the foreword of the present document) of the version of the supported 3GPP TS 31.113; BCD coded</p> <p>Byte 3: second digit (y according to the foreword of the present document) of the version of the supported 3GPP TS 31.113; BCD coded</p> <p>Bytes 4-5: Version of TS 31.114 [2] Byte 2: first digit (x according to the foreword of the present document) of the version of the supported 3GPP TS 31.114; BCD coded</p> <p>Byte 3: second digit (y according to the foreword of the present document) of the version of the supported 3GPP TS 31.114; BCD coded</p> <p>further bytes are RFU</p> <p>Example: Issuer version: '22' TS 31.113 version: 5.2.0 TS 31.114 version: 5.12.3 resulting coding: '22 05 02 05 12'</p>
'02'	USAT Command Filter	This includes the list of allowed USAT Commands. Coding as specified in TS 31.114 [2]. NOTE: Content is dynamic, i.e. it is impacted by the current configuration
'03'	USAT Interpreter Native Commands	List of supported native commands. Coding: Sequence of NCIs. Each NCI coded in 2 bytes.
'04'	Terminal Profile as got at runtime	Binary coded as defined in 3GPP TS 31.111 [1] for TERMINAL PROFILE
'05'	Error Code as generated by the last byte code command executed	Binary coded as specified in clause 12
'06'	Maximum page size for temporary storage of one page	Binary coded, most significant byte first: Number of bytes available for page storage.
'07'	USAT Interpreter issuer identification	URL of USAT Interpreter issuer, coding according to RFC 1738 [7] <host> of URL.
'08'	Hash Value of URL of USAT Interpreter issuer identification	4 most significant (left most) bytes of SHA-1 hash of the content of variable '07'
'09'	Reception Buffer Size	Binary coded, most significant byte first: – Receive buffer size in bytes available for messages to be received by the USAT Interpreter. This size includes all possibly needed space for transport headers, security, routing information, concatenation information and so on.
'0A'	USAT Interpreter Byte Code Filter	This includes the list of allowed USAT Interpreter byte codes. Coding as specified in TS 31.114 [2]. NOTE: Content is dynamic, i.e. it is impacted by the

		current configuration.
'0B'	Transmission Buffer Size	Binary coded, most significant byte first: - Transmit buffer size in bytes available for messages to be sent by the USAT Interpreter. This size includes all possibly needed space for transport headers, security, routing information, concatenation information and so on.
'0C'...'13'	RFU	

[...]

7.5 Inline Value

This TLV inserts a byte array, which often is simply running text, at the point of its appearance.

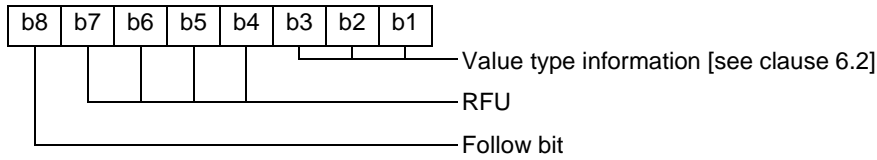
The Inline Value content may contain variable substitution indicators to indicate variable references. Therefore the Inline Value content has to be structured in Length-Value and Variable Substitution Indicator - Variable ID pairs. This structure shall be used even if the Inline Value content does not contain any variable substitution indicators. The possibly available constant data values and variable references have to be rendered according to clause 6.3 Method 1 during processing of this TLV by the USAT Interpreter. If the type of the possibly substituted variable values is different from the type indicated in the attribute of this TLV, the USAT Interpreter shall perform a type conversion or generate a "Type mismatch" error according to the following table:

from DCS	to DCS	comment
SMS default	SMS default	*
SMS packed		not supported, error generated
binary		cast allowed, no change of sequence of bytes
UCS2		not supported, error generated
unknown		cast allowed, no change of sequence of bytes
SMS default	SMS packed	not supported, error generated
SMS packed		*
binary		cast allowed, no change of sequence of bytes
UCS2		not supported, error generated
unknown		cast allowed, no change of sequence of bytes
SMS default	binary	cast allowed, no change of sequence of bytes
SMS packed		cast allowed, no change of sequence of bytes
binary		*
UCS2		cast allowed, no change of sequence of bytes
unknown		cast allowed, no change of sequence of bytes
SMS default	UCS2	conversion supplied, according to 3GPP TS 31.101 TS 402 221 [4]
SMS packed		not supported, error generated
binary		cast allowed, no change of sequence of bytes
UCS2		*
unknown		cast allowed, no change of sequence of bytes
SMS default	unknown	cast allowed, no change of sequence of bytes
SMS packed		cast allowed, no change of sequence of bytes
binary		cast allowed, no change of sequence of bytes
UCS2		cast allowed, no change of sequence of bytes
unknown		*

Coding of the Inline Value TLV:

Length	Value	Description	M/O
1	'0E' / '8E'	Inline Value Tag	M
1-3	A+B	Length	M
A	Data	Attributes	O
B	Data	Inline value content	O

Coding of the attributes:



If the value type information indicates "unknown", then the DCS attribute of the page shall be applied.

CHANGE REQUEST

⌘ **31.113 CR 028** ⌘ rev **-** ⌘ Current version: **6.2.0** ⌘

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 ME Radio Access Network Core Network

Title:	⌘ Correction of reference to SCP specification		
Source:	⌘ T3		
Work item code:	⌘ TEI	Date:	⌘ 18/11/2004
Category:	⌘ A	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> 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 .		<i>Use <u>one</u> of the following releases:</i> 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:	⌘ There was a discussion during TSG-T3 #32 on references to the SCP specifications, where if non-specific, it implies that later release features could be invoked into early release specifications by stealth (e.g. Rel-6 features into Rel-4 specifications by reference). To avoid this reference issue within the USAT Interpreter specifications, the reference to a SCP specification is replaced by a reference to the corresponding 3GPP specification.
Summary of change:	⌘ Reference to TS 102 221 is replaced by a reference to 3GPP TS 31.101.
Consequences if not approved:	⌘ Unclear usage of references.

Clauses affected:	⌘ 2, 6.1.1.1, 7.5										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
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 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 TS 31.111: "USIM Application Toolkit (USAT)".
- [2] 3GPP TS 31.114: "USAT Interpreter protocol and administration".
- [3] 3GPP TS 23.038: "Alphabets and language-specific information".
- [4] [3GPP TS 31.101](#): "~~ETSI TS 102 221~~: "~~Smart cards~~; UICC-~~t~~ Terminal interface; Physical and logical characteristics".
- [5] ISO/IEC 7816-6 (1995): "Identification cards – Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements".
- [6] void
- [7] IETF RFC 1738: "Uniform Resource Locators (URL)"
- [8] Schneier, Bruce: "Applied Cryptography Second Edition: Protocols, Algorithms and Source code in C", John Wiley & Sons, 1996, ISBN 0-471-12845-7.
- [9] RSA Laboratories: "PKCS #1 v2.0: RSA Cryptography Standard", www.rsasecurity.com/rsalabs/pkcs/
- [10] ISO/IEC 9797-1:1999(E): "Information technology – Security techniques – Message Authentication Codes (MACs)"
- [11] RSA Laboratories: "PKCS#9 v2.0: Selected Object Classes and Attribute Types", <http://www.rsasecurity.com/rsalabs/pkcs/>
- [12] FIPS PUB 180-1: "Secure Hash Standard (SHS)"
- [13] Wireless Application Forum: "Wireless Application Protocol – WMLScript Crypto Library Specification", Version 20-Jun-2001.
- [14] Wireless Application Forum: "Wireless Application Protocol – Wireless Transport Layer Security Specification", Version 18-Feb-2000.
- [15] IANA assigned character sets, <http://www.iana.org/assignments/character-sets>
- [16] RSA Laboratories: "PKCS #5 v2.0: Password-Based Cryptography Standard", <http://www.rsasecurity.com/rsalabs/pkcs/>
- [17] 3GPP TS 31.112: "USAT Interpreter Architecture Description; Stage 2"

[...]

6.1.1 Environment variable usage area

This usage area consists of 3 different partitions:

- USAT Interpreter system information partition;
- USIM issuer information partition;
- End user information partition.

6.1.1.1 USAT Interpreter system information partition

The USAT Interpreter partition is preloaded during the manufacturing process of the USIM or during the runtime of the USAT Interpreter.

At least the following information shall be stored:

Variable ID	Description	Coding
'00'	ICCID of UICC	Binary coding as for EF _{ICCID} specified in 3GPP TS 31.101 SCP TS 102-224 [4]
'01'	USAT Interpreter version	<p>Byte 1: Issuer Version USAT Interpreter issuer specific version. The coding and value of this byte depends on the USAT Interpreter issuer. The USAT Interpreter issuer is stored in variable '07' and variable '08'.</p> <p>Bytes 2-3: TS 31.113, Version (this TS) Byte 2: first digit (x according to the foreword of the present document) of the version of the supported 3GPP TS 31.113; BCD coded</p> <p>Byte 3: second digit (y according to the foreword of the present document) of the version of the supported 3GPP TS 31.113; BCD coded</p> <p>Bytes 4-5: Version of TS 31.114 [2] Byte 2: first digit (x according to the foreword of the present document) of the version of the supported 3GPP TS 31.114; BCD coded</p> <p>Byte 3: second digit (y according to the foreword of the present document) of the version of the supported 3GPP TS 31.114; BCD coded</p> <p>further bytes are RFU</p> <p>Example: Issuer version: '22' TS 31.113 version: 5.2.0 TS 31.114 version: 5.12.3 resulting coding: '22 05 02 05 12'</p>
'02'	USAT Command Filter	This includes the list of allowed USAT Commands. Coding as specified in TS 31.114 [2]. NOTE: Content is dynamic, i.e. it is impacted by the current configuration
'03'	USAT Interpreter Native Commands	List of supported native commands. Coding: Sequence of NCIs. Each NCI coded in 2 bytes.
'04'	Terminal Profile as got at runtime	Binary coded as defined in 3GPP TS 31.111 [1] for TERMINAL PROFILE
'05'	Error Code as generated by the last byte code command executed	Binary coded as specified in clause 12
'06'	Maximum page size for temporary storage of one page	Binary coded, most significant byte first: Number of bytes available for page storage.
'07'	USAT Interpreter issuer identification	URL of USAT Interpreter issuer, coding according to RFC 1738 [7] <host> of URL.
'08'	Hash Value of URL of USAT Interpreter issuer identification	4 most significant (left most) bytes of SHA-1 hash of the content of variable '07'
'09'	Reception Buffer Size	Binary coded, most significant byte first: – Receive buffer size in bytes available for messages to be received by the USAT Interpreter. This size includes all possibly needed space for transport headers, security, routing information, concatenation information and so on.
'0A'	USAT Interpreter Byte Code Filter	This includes the list of allowed USAT Interpreter byte codes. Coding as specified in TS 31.114 [2]. NOTE: Content is dynamic, i.e. it is impacted by the

		current configuration.
'0B'	Transmission Buffer Size	Binary coded, most significant byte first: – Transmit buffer size in bytes available for messages to be sent by the USAT Interpreter. This size includes all possibly needed space for transport headers, security, routing information, concatenation information and so on.
'0C'...'13'	RFU	

[...]

7.5 Inline Value

This TLV inserts a byte array, which often is simply running text, at the point of its appearance.

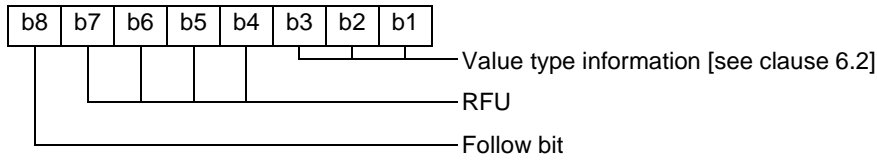
The Inline Value content may contain variable substitution indicators to indicate variable references. Therefore the Inline Value content has to be structured in Length-Value and Variable Substitution Indicator - Variable ID pairs. This structure shall be used even if the Inline Value content does not contain any variable substitution indicators. The possibly available constant data values and variable references have to be rendered according to clause 6.3 Method 1 during processing of this TLV by the USAT Interpreter. If the type of the possibly substituted variable values is different from the type indicated in the attribute of this TLV, the USAT Interpreter shall perform a type conversion or generate a "Type mismatch" error according to the following table:

from DCS	to DCS	comment
SMS default	SMS default	*
SMS packed		not supported, error generated
binary		cast allowed, no change of sequence of bytes
UCS2		not supported, error generated
unknown		cast allowed, no change of sequence of bytes
SMS default	SMS packed	not supported, error generated
SMS packed		*
binary		cast allowed, no change of sequence of bytes
UCS2		not supported, error generated
unknown		cast allowed, no change of sequence of bytes
SMS default	binary	cast allowed, no change of sequence of bytes
SMS packed		cast allowed, no change of sequence of bytes
binary		*
UCS2		cast allowed, no change of sequence of bytes
unknown		cast allowed, no change of sequence of bytes
SMS default	UCS2	conversion supplied, according to 3GPP TS 31.101 TS 402 221 [4]
SMS packed		not supported, error generated
binary		cast allowed, no change of sequence of bytes
UCS2		*
unknown		cast allowed, no change of sequence of bytes
SMS default	unknown	cast allowed, no change of sequence of bytes
SMS packed		cast allowed, no change of sequence of bytes
binary		cast allowed, no change of sequence of bytes
UCS2		cast allowed, no change of sequence of bytes
unknown		*

Coding of the Inline Value TLV:

Length	Value	Description	M/O
1	'0E' / '8E'	Inline Value Tag	M
1-3	A+B	Length	M
A	Data	Attributes	O
B	Data	Inline value content	O

Coding of the attributes:



If the value type information indicates "unknown", then the DCS attribute of the page shall be applied.