Technical Specification Group Services and System Aspects   **TSGS#19(03)0096**

Meeting #19, Birmingham, UK, 17-20 March 2003

Source:	**SA WG3**
Title:	**2 CRs to 33.108: Coding of ASN.1 parameters of the type OCTET STRING (Rel-5, Rel-6)**
Document for:	**Approval**
Agenda Item:	**7.3.3**

The following CRs were approved by SA WG3 meeting #27 and are hereby presented to TSG SA#19 for approval.

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-030096	33.108	007	-	Rel-5	Coding of ASN.1 parameters of the type OCTET STRING	F	5.2.0	SEC1-LI	S3-030094
SP-030096	33.108	008	-	Rel-6	Coding of ASN.1 parameters of the type OCTET STRING	A	6.0.0	SEC1-LI	S3-030095

3GPP TSG SA WG3 Security — S3#26
25 - 28 February 2003, Sophia Antipolis, France

S3-030094

3GPP TSG-SA3 LI Meeting 03/01
Paris, France, 19 – 21 February 2003

Tdoc ⌘ S3LI03_022r1

CR-Form-v7

CHANGE REQUEST

⌘	**33.108** CR **007**	⌘**rev**	**-**	⌘	Current version:	**5.2.0**	⌘

*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 ☒ **X**

Title:	⌘	Coding of ASN.1 parameters of the type OCTET STRING
Source:	⌘	SA3 LI

Work item code: ⌘	SEC1-LI		*Date:* ⌘	20.02.2003

Category:	⌘	**F**	*Release:* ⌘	Rel-5

Use <u>one</u> 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 <u>one</u> of the following releases:
   2   *(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)*

Reason for change: ⌘	In the current text of TS 33.108, nowhere the ordering of the individual nibbles of each octet is specified. Usually, the ordering is such that the least significant nibble is put into bitposition 1-4 and the most significant nibble into bitposition 5-8, as it is e.g. the case for the representation of ASCII characters. However, in some standards, see e.g. the Calling Party Number in ISUP, which is referenced in TS 33.108, the order is such that the most significant nibbles (BCD coded digits of the E.164 number) are put into bitposition 1-4 and the least significant nibble is put into bitposition 5-8.
	As we have seen implementations where the latter rule has been applied also for other ASN.1 parameters of the type OCTET STRING, we feel it necessary to insert a statement specifying the general rule into the introduction part of the ASN.1 description in Annex B of TS 33.108.
Summary of change: ⌘	In order to avoid divergent implementations, the ordering of the nibbles in each octet of the ASN.1 parameters of the type OCTET STRING should be specified.
Consequences if not approved: ⌘	Possibly divergent implementations
Clauses affected: ⌘	Annex B

Other specs affected:	⌘	Y	N		⌘	
			X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

2 References

[29]   ITU-T Recommendation Q.763: " Formats_and_Codes_of the_ISDN_User_Part_of_Signalling_System No._7".

B.1   Syntax definitions

The transferred information and messages are encoded to be binary compatible with [5] (Abstract Syntax Notation One (ASN.1)) and [6] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type,* in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [5] and [6]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely use a standardized format when it exists (ISUP, DSS1, MAP, …).

As a large part of the information exchanged between the user's may be transmitted within ISUP/DSS1 signalling, the using of the coding defined for this signalling guarantee the integrity of the information provided to the LEMF and the evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

For the ASN.1 parameters of the type 'OCTET STRING', the ordering of the individual halfoctets of each octet shall be such that the most significant nibble is put into bitposition 5 – 8 and the least significant nibble into bitposition 1 – 4. This general rule shall not apply when parameter formats are imported from other standards, e.g. an E.164 number coded according to ISUP [29]. In this case the ordering of the nibbles shall be according to that standard and not be changed.

Annex E (informative):
Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

1.	ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

2.	EN 300 356-1 to -20: "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface; Parts 1 to 20".

3.	EN 300 403-1 (V1.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

4.	EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

5.	EN 300 097-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

6.	EN 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

7.	EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

8.	EN 300 138-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

9.	EN 300 185-1: "Integrated Services Digital Network (ISDN); Conference call, add-on (CONF) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

10.	ETS 300 188-1: "Integrated Services Digital Network (ISDN); Three-Party (3PTY) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

11.	EN 300 207-1 (V1.2): "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

12.	EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

13.	EN 300 369-1 (V1.2): "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

14.	EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

15.	ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

16.	ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

17.	ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

18. EN 300 122-1: "Integrated Services Digital Network (ISDN); Generic keypad protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

19. ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

20. EN 301 344, GSM 03.60: "Digital cellular telecommunications system (Phase 2+); GPRS Service description stage 2".

21. RFC-2228: "FTP Security Extensions", October 1997.

22. ITU-T Recommendation Q.763: "Signalling System No.7 - ISDN User Part formats and codes".

23. ETSI TR 101 876 "Telecommunications security; Lawful Interception (LI); Description of GPRS HI3".

3GPP TSG SA WG3 Security — S3#26
25 - 28 February 2003, Sophia Antipolis, France

S3-030095

3GPP TSG-SA3 LI Meeting 03/01
Paris, France, 19 – 21 February 2003

Tdoc ⌘ S3LI03_023r1

CR-Form-v7

CHANGE REQUEST

⌘	**33.108** CR **008**	⌘**rev**	**-**	⌘	Current version:	**6.0.0**	⌘

*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 **X**

Title: ⌘	Coding of ASN.1 parameters of the type OCTET STRING	
Source: ⌘	SA3 LI	
Work item code: ⌘	SEC1-LI	***Date:*** ⌘ 20.02.2003
Category: ⌘ **A**		***Release:*** ⌘ Rel-6

Use <u>one</u> 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 <u>one</u> of the following releases:
  2   *(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)*

Reason for change: ⌘	In the current text of TS 33.108, nowhere the ordering of the individual nibbles of each octet is specified. Usually, the ordering is such that the least significant nibble is put into bitposition 1-4 and the most significant nibble into bitposition 5-8, as it is e.g. the case for the representation of ASCII characters. However, in some standards, see e.g. the Calling Party Number in ISUP, which is referenced in TS 33.108, the order is such that the most significant nibbles (BCD coded digits of the E.164 number) are put into bitposition 1-4 and the least significant nibble is put into bitposition 5-8. As we have seen implementations where the latter rule has been applied also for other ASN.1 parameters of the type OCTET STRING, we feel it necessary to insert a statement specifying the general rule into the introduction part of the ASN.1 description in Annex B of TS 33.108.
Summary of change: ⌘	In order to avoid divergent implementations, the ordering of the nibbles in each octet of the ASN.1 parameters of the type OCTET STRING should be specified.
Consequences if not approved: ⌘	Possibly divergent implementations
Clauses affected: ⌘	Annex B

	Y	N		
Other specs ⌘		X	Other core specifications ⌘	
affected:		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘	

2 References

[29]   ITU-T Recommendation Q.763: " Formats and Codes of the ISDN User Part of Signalling System No. 7".

B.1   Syntax definitions

The transferred information and messages are encoded to be binary compatible with [5] (Abstract Syntax Notation One (ASN.1)) and [6] (Basic Encoding Rules (BER)).

These recommendations use precise definitions of the words *type*, *class*, *value*, and *parameter*. Those definitions are paraphrased below for clarity.

A *type,* in the context of the abstract syntax or transfer syntax, is a set of all possible values. For example, an INTEGER is a type for all negative and positive integers.

A *class*, in the context of the abstract syntax or transfer syntax, is a one of four possible domains for uniquely defining a type. The classes defined by ASN.1 and BER are: UNIVERSAL, APPLICATION, CONTEXT, and PRIVATE.

The UNIVERSAL class is reserved for international standards such as [5] and [6]. Most parameter type identifiers in the HI ROSE operations are encoded as CONTEXT specific class. Users of the protocol may extend the syntax with PRIVATE class parameters without conflict with the present document, but risk conflict with other users' extensions. APPLICATION class parameters are reserved for future extensions.

A *value* is a particular instance of a type. For example, five (5) is a possible value of the type INTEGER.

A *parameter* in the present document is a particular instance of the transfer syntax to transport a value consisting of a tag to identify the parameter type, a length to specify the number of octets in the value, and the value.

In the BER a *tag* (a particular type and class identifier) may either be a primitive or a constructor. A *primitive* is a pre-defined type (of class UNIVERSAL) and a *constructor* consists of other types (primitives or other constructors). A constructor type may either be IMPLICIT or EXPLICIT. An IMPLICIT type is encoded with the constructor identifier alone. Both ends of a communication must understand the underlying structure of the IMPLICIT types. EXPLICIT types are encoded with the identifiers of all the contained types. For example, an IMPLICIT Number of type INTEGER would be tagged only with the *Number* tag, where an EXPLICIT number of type INTEGER would have the *INTEGER* tag within the *Number* tag. The present document uses IMPLICIT tagging for more compact message encoding.

For the coding of the value part of each parameter the general rule is to use a widely use a standardized format when it exists (ISUP, DSS1, MAP, …).

As a large part of the information exchanged between the user's may be transmitted within ISUP/DSS1 signalling, the using of the coding defined for this signalling guarantee the integrity of the information provided to the LEMF and the evolution of the interface. For example if new values are used within existing ISUP parameters, this new values shall be transmitted transparently toward the LEMF.

For the ASN.1 parameters of the type 'OCTET STRING', the ordering of the individual halfoctets of each octet shall be such that the most significant nibble is put into bitposition 5 – 8 and the least significant nibble into bitposition 1 – 4. This general rule shall not apply when parameter formats are imported from other standards, e.g. an E.164 number coded according to ISUP [29]. In this case the ordering of the nibbles shall be according to that standard and not be changed.

Annex E (informative):
Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

1.   ITU-T Recommendation X.25: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit".

2. EN 300 356-1 to -20: "Integrated Services Digital Network (ISDN); Signalling System No.7; ISDN User Part (ISUP) version 3 for the international interface; Parts 1 to 20".

3. EN 300 403-1 (V1.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

4. EN 300 061-1: "Integrated Services Digital Network (ISDN); Subaddressing (SUB) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

5. EN 300 097-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Connected Line Identification Presentation (COLP) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

6. EN 300 098-1: "Integrated Services Digital Network (ISDN); Connected Line Identification Restriction (COLR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

7. EN 300 130-1: "Integrated Services Digital Network (ISDN); Malicious Call Identification (MCID) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

8. EN 300 138-1 including Amendment 1: "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

9. EN 300 185-1: "Integrated Services Digital Network (ISDN); Conference call, add-on (CONF) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

10. ETS 300 188-1: "Integrated Services Digital Network (ISDN); Three-Party (3PTY) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

11. EN 300 207-1 (V1.2): "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

12. EN 300 286-1: "Integrated Services Digital Network (ISDN); User-to-User Signalling (UUS) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

13. EN 300 369-1 (V1.2): "Integrated Services Digital Network (ISDN); Explicit Call Transfer (ECT) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

14. EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

15. ITU-T Recommendation Q.850: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

16. ITU-T Recommendation X.881: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) service definition".

17. ITU-T Recommendation X.882: "Information technology - Remote Operations: OSI realizations - Remote Operations Service Element (ROSE) protocol specification".

18. EN 300 122-1: "Integrated Services Digital Network (ISDN); Generic keypad protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

19.   ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

20.   EN 301 344, GSM 03.60: "Digital cellular telecommunications system (Phase 2+); GPRS Service description stage 2".

21.   RFC-2228: "FTP Security Extensions", October 1997.

22.   ITU-T Recommendation Q.763: "Signalling System No.7 - ISDN User Part formats and codes".

23.   ETSI TR 101 876 "Telecommunications security; Lawful Interception (LI); Description of GPRS HI3".