3GPP TSG SA WG3 Security — S3#21 **S3-010661**

27 - 30 November, 2001

Sophia Antipolis, France

3GPP TSG CN WG5 Meeting #14 **N5-011159**
Meeting #15, Cancun, MEXICO, 26 – 30 November 2001

Title:	**Liaison Statement on the Support of Up to Date Encryption Algorithms in the OSA Framework**
Source:	**CN5**
To:	**SA3**
Cc:	
Response to:	LS (S3-010574 / N5-011113) on "Comments to TS 29.198" from WG SA3.

Contact Person:

Name: **Musa Unmehopa, CN5 vice chair**
Tel. Number: +31 35 687 1684
E-mail Address: unmehopa@lucent.com

Name: **Adrian Zoicas, CN5 MCC**
Tel. Number: +33 6 74 40 83 72
E-mail Address: Adrian.Zoicas@etsi.fr

Attachments: N5-011152 Change Request to 3GPP TS 29.198-03

---

1. Overall Description:

CN5 thanks SA3 for their Liaison Statement containing review comments to the encryption algorithm sections in the OSA Framework specification 3GPP TS 29.198-03 v4.2.0.

It is important to note that the OSA specifications do not mandate the use of any specific encryption algorithm, nor is it the intention to restrict the possible encryption algorithms to some specific subset. The method selectEncryptionMethod in the IpAPILevelAuthentication interface is used to select an encryption algorithm that is used to encrypt the challenge that is passed in the authenticate method of the IpClientAPILevelAuthentication interface. The selectEncryption method takes parameter encryptionCaps of type TpEncryptionCapabilityList as input.

In order to cater for the comments that SA3 raised in their LS S3-010574, CN5 proposes to enhance the encryption algorithm data type, TpEncryptionCapability, to include the more up to date encryption algorithms proposed by SA3. CN5 proposes to maintain the existing enumeration values for reasons of backward compatibility. This proposal is attached to this Liaison Statement, as document N5-011152.

A brief but non-exhaustive literature search has been performed to obtain the correct external references to the encryption standards proposed by SA3. This search has shown that of the examples provided in LS S3-010574 the AES (Advanced Encryption Standards), also referred to as Rijndael, is not yet standardized. Although publication of this standard is imminent, CN5 feels it is inappropriate to reference non-standardized algorithms. In addition, no standards specification for the RIPE-MD160 was found as a result of the brief search. CN5 would like to point out that it is still possible to use the AES and RIPE-MD160 encryption algorithms using the 3GPP TS 29.198-03 specification. The following is a caption from the data definition of TpEncryptionCapability:

> This data type is identical to a TpString, and is defined as a string of characters that identify the encryption capabilities that could be supported by the framework. Other Network operator specific capabilities may also be used, but should be preceded by the string "SP_".

So for instance operator specific strings "SP_AES" and "SP_RIPE_MD_160" can be passed between the client application and the OSA Framework.

CN5 is currently meeting in Cancun from 26-30 November 2001 (-7 hours to CET). The present CN5 meeting could approve the attached CR in N5-011152 for inclusion in the Rel-4 OSA stage 3 specification 29.198, in the event SA3 provides a reply to this LS before the close of the CN5 meeting on Friday 30 November 2001. CN5 would like to submit this CR to the Kyoto plenary (CN#14) in two weeks from now.

2. Actions:

To SA3 group.

ACTION: CN5 asks SA3 to review and approve the proposed updates to the security algorithm data types in the OSA Framework specification, specified in attachment N5-011152. CN5 would like to point out that in order for these changes to make it into Release 4, **an answer is required this week, Friday the 30th at the latest**. Therefore CN5 would like to kindly request SA3 for a reply to this Liaison Statement at their earliest convenience, though no later than the closing of the ongoing CN5#15 meeting at Friday November the 30th.

3. Date of Next CN5 Meetings:

CN5_16	4 – 8 February 2002	Hong Kong, CHINA

3GPP TSG_CN5 (Open Service Access – OSA) **N5-011152**
Meeting #15, Cancun, MEXICO, 26 – 30 November 2001

CR-Form-v4

CHANGE REQUEST

⌘ **29.198-03** **CR** **CRNum** ⌘ ev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Enhance data type TpEncryptionCapability to include more up to date, higher grade, encryption algorithms to encrypt the challenge that is used to authenticate OSA client applications with the Framework
Source:	⌘	Lucent Technologies
Work item code:	⌘	OSA1
Date:	⌘	16/11/2001
Category:	⌘	**F**
Release:	⌘	Rel-4

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:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	The encryption capabilities currently supported to authenticate an OSA client application with the OSA Framework are low-grade and outdated.
Summary of change:	⌘	Enhancing the TpEncryptionCapability data type with high-grade, up to date encryption capabilities.
Consequences if not approved:	⌘	If not approved, the authentication process between OSA client application and the OSA Framework can be compromised.

Clauses affected:	⌘	2, 10.3.3
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ 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/3G_Specs/CRs.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 29.198-1 "Open Service Access; Application Programming Interface; Part 1: Overview".

[2] 3GPP TS 22.127: "Stage 1 Service Requirement for the Open Service Access (OSA) (Release 4)".

[3] 3GPP TS 23.127: "Virtual Home Environment (Release 4)".

[4] IETF PPP Authentication Protocols - Challenge Handshake Authentication Protocol [RFC 1994, August1996].

[5] The Digital Encryption Standard (DES), National Institute of Standards and Technology, NIST FIPS PUB 46-3, Federal Information processing Standards Publication 46-3 Digital Encryption Standard, 25 October 1999.

[6] Public Key Cryptography Standard #1, v2.0: RSA Cryptography Standard, http://www.rsa.com/rsalabs/pkcs/pkcs-1/index.html

[7] The Secure Hash Algorithm (SHA-1), National Institute of Standards and Technology, NIST FIPS PUB 180-1, Federal Information processing Standards Publication 180-1 Secure Hash Standard, 17 April 1995.

[8] The Digital Signature Algorithm (DSA), National Institute of Standards and Technology, NIST FIPS PUB 186-2, Federal Information Processing Standards Publication 186-2 Digital Signature Standard (DSS), 27 January 2000

10.3.3 TpEncryptionCapability

This data type is identical to a TpString, and is defined as a string of characters that identify the encryption capabilities that could be supported by the framework. Other Network operator specific capabilities may also be used, but should be preceded by the string "SP_". Capabilities may be concatenated, using commas (,) as the separation character. The following values are defined.

String Value	Description
NULL	An empty (NULL) string indicates no client capabilities.
P_DES_56	A simple transfer of secret information that is shared between the client application and the Framework with protection against interception on the link provided by the DES algorithm with a 56-bit shared secret key. [5]
P_DES_112	A simple transfer of secret information that is shared between the client application and the Framework with protection against interception on the link provided by the DES algorithm with a 2x56=112-bit shared secret key. Referred to as triple DES [5]
P_DES_128	A simple transfer of secret information that is shared between the client entity and the Framework with protection against interception on the link provided by the DES algorithm with a 128-bit shared secret key. [5]
P_RSA_512	A public-key cryptography system providing authentication without prior exchange of secrets using 512-bit keys [6].
P_RSA_1024	A public-key cryptography system providing authentication without prior exchange of secrets using 1024-bit keys [6].
P_SHA_1	Secure Hash Algorithm, a cryptographic message digest algorithm using a 160-bit message digest [7].
P_DSA	Digital Signature Algorithm, a cryptographic message digest algorithm using a 160-bit message digest [8].