3GPP TSG SA WG3 Security — SA3#36 **S3-041047**
November 23-26, 2004
Shenzhen, China

3GPP TSG-CN WG4 Meeting #25 **N4-041605**
Seoul, KOREA. 15th to 19th November 2004.

Title:	**Reply LS on Security aspects of early IMS systems**
Response to:	**LS (S3-040880) on Security aspects of early IMS systems from SA3**
Source:	**CN4**
To:	**SA3**

Contact Person:
Name: Dan Warren, Vodafone
Tel. Number: +44 7795 300783
E-mail Address: dan.warren@vodafone.com

Attachments: N4-041643 - CN4 impacts of Early IMS security mechanisms.

1. Overall Description:

CN4 thanks SA3 for their LS in S3-040880 (N4-0401265) on Security aspects of early IMS systems. CN4 considered the attached TR33.878 and have identified a number of impacts on the current specification of Cx interface within 3GPP TS 29.228 and 3GPP TS 29.229. These have been documented in the attached document, N4-041643.

CN4 was not able to decide where best to document the information included in N4-041643. Whilst the information is relevant to Cx interface and so could be incorporated in TS 29.228, it seemed inappropriate to do this when the intention of Early IMS Security is to be something that is used early in IMS deployment, whilst 29.228 is the normative description of Cx interface support of full IMS security. If it were included in 29.228, it would form an informative Annex and would only be included in the R6 specifications. Alternatively, the information could be included in TR 33.878 in a new section. This may seem appropriate and would result in the full detail of the Early IMS Security implementation being held in a single document, if a similar approach were adopted by other groups handling stage 3 details.

CN4 has a preference for the inclusion of this information in TR33.878, but asks SA3 to decide where the documentation of Cx impacts as a result of Early IMS Security is best addressed.

2. Actions:

To SA3 group.

ACTION: CN4 asks SA3 to consider the information within N4-041643 and either to include it within TR33.878 or inform CN4 that the content of N4-041643 should be added to 29.228.

3. Date of Next CN4 Meetings:

CN4#26	14th - 18th February 2004	Sydney, AUSTRALIA
CN4#27	25th - 29th April 2004	Cancun, MEXICO

3GPP TSG-CN WG4 Meeting #25 **N4-041643**
Seoul, KOREA. 15th to 19th November 2004.

Source: **Vodafone**

Title: **Cx interface implementation for Early IMS Security**

Agenda item: **7.17.2**

Document for: **Approval**

The definition of Early IMS Security mechanisms is being completed by SA3 as indicated in N4-041265. In order for the Early IMS Security approach to be completed, Cx interface implementation needs to be defined to carry alternative parameters.

This document identifies the differences that are required for the Cx interface. These need to be documented either in the Early IMS Security TR (TR 33.878 under SA3 control) or within an informative Annex in the Cx interface specification (TS 29.228 under CN4 control). The decision on where this content is best handled is to be made by SA3.

Impact of Early IMS Security on Cx Interface

Early IMS Security mechanism affects the use of the protocol defined for the Cx interface. In particular, the User-Authorisation-Request and Multimedia-Auth-Request/Answer messages are impacted.

Because in Early IMS Security the Private User Identity of the subscriber is not made available to the IMS domain in SIP messages, it is necessary to derive a Private User Identity from the Temporary Public User Identity to use as the content of the User-Name AVP in certain Cx messages (most notable UAR and MAR).

1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in 6.1.1 of 3GPP TS 29.228 [x], with the following exception;-

- the Private User Identity (User-Name AVP) in the UAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present port number, URI parameters, and headers

2 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in 6.3 of 3GPP TS 29.228 [x] of this document, with the following exceptions;-

- the Private User Identity (User-Name AVP) in the MAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and headers.

- In the MAR and MAA commands, the Authentication Scheme (Authentication-Scheme AVP described in section 7.9.2 of 3GPP TS 29.228 [x]) within the SIP-Auth-Data-Item grouped AVP shall contain "Early-IMS-Security".

- In the MAA command, the SIP-Auth-Data-Item grouped AVP shall contain the user IP address. If the address is IPv4 it shall be included within the Framed-IP-Address AVP as defined in draft-ietf-aaa-diameter-nasreq-17.txt [y]. If the address is IPv6 it shall be included within the Framed-IPv6-Prefix AVP and, if the Framed-IPv6-Prefix AVP alone is not unique for the user it shall also contain Framed-Interface-Id AVP.

  This results in SIP-Auth-Data-Item as depicted in table 6.3.4 of 3GPP TS 29.228 [x], being replaced when Early IMS Security is employed by a structure as shown in table 2.1;-

Table 2.1: Authentication Data content for Early IMS Security – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For Early IMS Security it will indicate “Early-IMS-Security”
User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].
Framed Interface Id	Framed-Interface-Id	C	If the IP Address of the User is an IPv6 address and the Framed-IPv6-Address AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].

The ABNF description of the AVP as given in section 6.3.13 of 3GPP TS 29.229 [z] is replaced with that given below.

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >
      [ SIP-Authentication-Scheme ]
      [ Framed-IP-Address ]
      [ Framed-IPv6-Prefix ]
      [ Framed-Interface-Id ]
      * [AVP]
```

- Step 5 of section 6.3.1 of this document shall apply with the following exception:
    - HSS shall return only one SIP-Auth-Data-Item

References

[x] 3GPP TS 29.228: ““IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents”

[y] IETF draft ‘draft-ietf-aaa-diameter-nasreq-17.txt’

[z] 3GPP TS 29.229: “Cx Interface based on Diameter – Protocol details”