3GPP TSG CN Plenary Meeting #25 **NP-040391**
8th – 10th September 2004 palm Springs, CA, US

Source: TSG CN WG4

Title: Liaison statements after CN#24

Agenda item: 6.4.1

Document for: INFORMATION

Tdoc	Tdoc Title	LS to	LS cc	LS Attachment
N4-040834	Authorization Logic and the Entities Involved	SA2		
N4-040848	LS on On-line charging Disconnection Procedure	SA2		
N4-040855	LS on use of MSISDN in WLAN-AN	SA5		
N4-041111	Reply LS on the flexibility of filtering of register request	SA2 CN1		N4-041100 N4-041116
N4-041115	LS on mapping of cause codes for no radio resources available and for load higher in target cell	RAN3 GERAN2		N4-040901 N4-040892
N4-041123	LS Response on LS on Assignment of the Diameter codes and identifiers	SA5		
N4-041133	LS on RIM transparent routing	RAN3 GERAN2 SA2		N4-041132
N4-041166	LS on Generic Authentication Architecture (GAA)	SA2	SA3	
N4-041192	Renumbering of 3GPP specific AVP codes	SA5		N4-041210
N4-041193	LS on 'SMS Fraud countermeasures	SA3	T2	N4-040959
N4-041201	Output LS on Supporting RADIUS/DIAMETER Protocol at Wd Interface	SA2	SA5	
N4-041202	LS on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements	SA3		
N4-041203	Reply LS on Clarification of TMGI format	SA1, RAN2	SA2, CN1	
N4-041204	LS on Evaluation of the alternatives for SMS fraud countermeasures	GSM-A IREG, GSM-A SG	SA3	

3GPP TSG CN WG4 Meeting #23bis ***N4-040834***
Helsinki, FINLAND, 21st – 23rd JUNE 2004

Title: Authorization Logic and the Entities Involved.
Release: Release 6
Work Item: GUP

Source: CN4
To: SA2
Cc:

Contact Person:
Name: Arnaud SAHUGUET (Lucent Technologies)
Tel. Number: +1 908 582 6491
E-mail Address: sahuguet@research.bell-labs.com

Attachments: None

---

1. Overall Description:

In the current SA2 GUP stage 2 document, the authorization is the responsibility of the GUP server and the RAF: "The GUP Server shall take care of the authorization of the access to the user profile data. The authorization itself may be handled by a separate entity in the network, or alternatively by the RAF or GUP Data Repository."

In most cases, authorization involves some complicated authorization logic that involves some context information such as requestor identity, purpose of the request, etc.

It appears to CN4 that having both GUP server and RAF handle authorization creates an un-needed complication and will result in some overhead.

The advantages of a solution where the authorization logic is only handled by the GUP servers have the following advantages.

- Simplicity
  Authorization logic and authorization data are only handled by one entity. RAF implementations do not need to implement authorization logic and interfaces.

- Consistency
  Having authorization logic and authorization data handled by one entity avoids conflicts or inconsistencies (e.g. conflicting authorization rules available at different RAFs). This is also more in-line with the "single point of access" philosophy of GUP.

- Overload avoided at the RAF
  This proposal reduces the functionality of the RAF to a strict minimum which is valuable, since the RAF is going to live next to core network components,

- More efficient in terms of bandwidth
  Authorization decisions require some context information (e.g. purpose of the request, etc.). In the case where the authorization logic is handled by the GUP server and by the RAF, messages containing context information needs to be passed to both.

During CN4 internal discussions related to this issue, two important-use cases related to this change have been raised. CN4 wishes to share with SA2 how the proposal addresses these the following two important cases: (1) non-proxy mode and (2) visited network.

1. Use case: GUP server in non proxy mode

In the case where the GUP server does not behave according to the proxy mode, authorization can be handled as follows. The application sends a request to the GUP server.

The GUP server performs the authorization logic and rewrites the request accordingly. The request is signed by the GUP server (using any form of cryptographic certificate).

The signed request is sent back to the application. The application forwards the request to the corresponding RAF. The RAF checks that the signature corresponds to the GUP server. If the check fails, the request is denied. If the check is valid, the data is sent back to the application.

2. Use case: Visited Network application

As defined in TS 23.240, visited network applications will access Home Network GUP data through the Home Network GUP server. The Home Network GUP server will apply the authorization logic for inter network authorization policies.

2. Actions:

To SA2 group.

ACTION:

CN4 kindly asks the opinion of SA2 on the proposal where the authorization logic would be only handled by the GUP server but could be applied in the RAF by the means explained above. CN4 does not see any conflict with the current TS 23.240 but seeks clarification that the intended architectural requirements are fulfilled by the mechanisms proposed by CN4.

3. Date of Next CN4 Meeting:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	Pusan, South-Korea

3GPP TSG CN WG4 Meeting #23bis ***N4-040848***
Helsinki, FINLAND, 21st – 23rd JUNE 2004

Title: LS on On-line charging Disconnection Procedure
Response to:
Release: Rel-6.
Work Item: WLAN

Source: CN4
To: SA2
Cc:

Contact Person:
Name: Maria-Carmen Belinchon
Tel. Number: +34 91 339 3535
E-mail Address: maria.carmen.belinchon@ericsson.com

Attachments:

---

1. Overall Description:

Section 7.3 in TS 23.234 indicates that when a user is disconnected by the OCS system due to credit request denial, the 3GPP AAA Server informs the HSS by Wx procedures that the WLAN registration for the user in the 3GPP AAA server has been cancelled.

CN4 would like to ask guidance to SA2 on the way that the 3GPP AAA Server should perform such a notification. A question has been raised in CN4 whether the 3GPP AAA Server should clearly indicate in the de-registration notification that the cause is on-line charging failure, i.e., whether or not the HSS is expected to perform any specific action when receiving a de-registration notification due to on-line failure. Otherwise CN4 shall use a general de-registration code.

2. Actions:

To SA2 group.

ACTION: CN4 kindly asks SA2 to provide an answer on the question raised above.

3. Date of Next CN4 Meeting:

CN4 #24	16th – 20th August 2004	Sophia Antipolis, FRANCE
CN4 #25	15th – 19th November 2004	Pusan, South-Korea

3GPP TSG CN WG4 Meeting #23bis N4-040855
Helsinki, Finland, 21th – 23rd June 2004

Title: LS on use of MSISDN in WLAN-AN
Release: Release 6
Work Item: WLAN

Source: CN4
To: SA5
Cc:

Contact Person:
Name: Paul Sitch
Tel. Number: +1 650 996 3742
E-mail Address: paul.sitch@nokia.com

Attachments: None

---

1. Overall Description:

CN4 is aware that MSISDN shall be used at the VPLMN as an identity for charging purposes. CN4 seek further clarification as to whether the MSISDN may also be used at the WLAN-AN for charging purposes.

2. Actions:

To SA5 group.

ACTION: Clarify the above point

3. Date of Next TSG-CN4 Meetings:

TSG-CN4 Meeting 24	16th -20th August 2004	Sophia Antipolis .
TSG-CN4 Meeting 25	15th -19th November	Pusan, South Korea

3GPP TSG-CN4 Meeting #24 Tdoc N4-041111
Sophia Antipolis, France 16th – 20th August 2004

Title: Reply LS on the flexibility of filtering of register request
Response to: LS (S2-042280) and (N1-041314) on LS on the flexibility of filtering of register request
Release: Release 6
Work Item: IMS2

Source: CN4
To: SA2, CN1

Contact Person:
Name: John Fenn
Tel. Number: +44 7879642149
E-mail Address: jfenn@rim.com
Attachments: N4-041100 and N4-041116

---

1. Overall Description:

CN4 thanks SA2 and CN1 for their liaison statements on the flexibility of filtering of register request.

CN4 have in response to this liaison agreed the attached CRs to their specifications. CN4 determined that the best solution was to define a new SPT attribute "RegistrationType" having the values INITIAL_REGISTRATION, RE-REGISTRATION, and DE-REGISTRATION instead of extending the Session Case entry values as proposed in N1-041310.

CN4 understand that a corresponding CR to TS 23.218 has been submitted to CN1.

2. Actions:

To CN1 group.

ACTION:

Consider the changes in the attached CRs and make the corresponding changes to TS 23.218.

3. Date of Next TSG-CN4 Meetings:

CN4_25	15th – 19th November 2004	Seoul, Korea

3GPP TSG-CN WG4 Meeting #24 **N4-041115**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: LS on New Cause Code in RANAP for "Traffic load in the target cell higher than in the source cell"
Response to: LS R3-040942 and GP-041727
Release:
Work Item:

Source: **CN4**
To: **RAN3, GERAN2**
Cc:

Contact Person:
Name: phil hodges
Tel. Number: +61404069546
E-mail Address: Philip.hodges@ericsson.com

Attachments: N4-040901, N4-040892

---

1. Overall Description:

CN4 thank GERAN2 and RAN3 for their liaison statements (enclosed) regarding the need for a new causecode in RANAP for the Traffic load in the target cell higher than in the source cell. As CN4 initiated this question as a result of trying to improve the error mapping between GERAN and RANAP it was felt that CN4 should reconsider this issue and respond to your WGs. Having considered the responses from both groups CN4 has agreed that we do not wish to mandate a new causecode in RANAP and CN4 should update the TS 29.010 taking into account the proposals from RAN3.

2. Actions:

To RAN3 group.

ACTION: CN4 asks RAN3 group to disregard our previous request to consider adding a new causecode for the above-described case.

3. Date of Next CN3 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041123**
Sophia Antipolis, France. 16th to 20th August 2004.

Title:	Response on LS on Assignment of the Diameter codes and identifiers
Response to:	LS (N4-040919) on Assignment of the Diameter codes and identifiers from SA5
Release:	Rel-6
Work Item:	-
Source:	CN4
To:	SA5
Cc:	-

Contact Person:
Name: Maria-Carmen Belinchon
Tel. Number: +34 91 3393535
E-mail Address: maria.Carmen.belinchon@ericsson.com

Attachments: -

---

1. Overall Description:

CN4 would like to thank SA5 for the review of the TS 29.230 and their concerns raised in LS on "Assignment of the Diameter codes and identifiers". CN4 would like to clarify the question raised by SA5 regarding Annex A.3/A.4:

> **Annex A.3/A.4**: SA5 would like to have the same procedure for AVP codes and result codes as for Application Ids and Command codes. If so all AVP codes and Result codes will be specified only in one specification in order to avoid inconsistency. If CN4 handles all Application Ids, Command codes, AVP codes and result codes then SA5 don't require a response LS on our requests. Instead TS 32.299 will not include any codes, but refer to TS 29.230 for this information.

AVPs needs to be listed within each specification since it is needed a place where the AVP is defined and since each specification should contain a table to indicate the nature of the AVPs, i.e., the flags, types and encryptation, as it is defined by IETF RFC 3588 and has been implemented within existing 3GPP Cx and Sh specifications (TS 29.229 and TS 29.239).

CN4 would like to clarify that TS 29.230 lists the ranges of codes assigned by either IANA or 3GPP to Diameter Application-Ids, Command Codes, AVPs and Experimental Result Codes, but does not define the meaning of such elements and should be done within the specification that applied for the code.

2. Actions:

To SA5 group.

ACTION: CN4 asks SA5 group to note the above and proceed accordingly within the Diameter specifications.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041133**
Sophia Antipolis, France. 16th to 20th August 2004.

Title:	**LS on RIM routing addressing between GERAN and UTRAN**
Response to:	LS on 'RIM Routing Addressing between GERAN and UTRAN' (**R3-040568 & GP-040443)**
Release:	Release 6
Work Item:	RANimp-NACC
Source:	**CN4**
To:	TSG GERAN WG2, TSG RAN3 & TSG SA2
Cc:	

Contact Person:
Name: Richard Brook
Tel. Number: +44 1628 432033
E-mail Address: mailto:rbrook@nortelnetworks.com

Attachments: N4-041132

---

1. Overall Description:

CN4 would like to thank GERAN WG2 for their LS initiating this issue and RAN 3 for their guidance on the coding of the proposed information element.

CN 4 have approved the attached CR to 29.060.

A concern was raised in CN 4 as to whether this change to 29.060 would have an impact on 23.060 and so asks SA 2 to look into this and if so make the appropriate change.

2. Actions:

To SA 2 group.

ACTION: CN3 asks SA 2 group to check whether any change is required to 23.060 by this change to 29.060?

If this is so then SA 2 is asked to make the appropriate change.

3. Date of Next CN3 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041166**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: LS on Generic Authentication Architecture (GAA)
Response to: -
Release: Rel-6
Work Item: -

Source: CN4
To: SA2
Cc: SA3

Contact Person:
Name: Maria-Carmen Belinchon
Tel. Number: +34 91 3393535
E-mail Address: maria.carmen.belinchon@ericsson.com

Attachments: -

---

1. Overall Description:

CN4 is currently defining the Generic Authentication Architecture (GAA) parameters to be stored within the HSS. While doing this, it was discussed whether Generic Authentication Architecture (GAA) should be considered as a new domain, different from CS/PS and IMS, or should instead be considered as a feature within the aforementioned domains.

CN4 opinion is that SA2 should define such an architectural issue so that CN4 can then define how these data are stored/retrieved within/from the HSS.

2. Actions:

To SA2 group.

ACTION: CN4 asks SA2 to provide guidance on the above issue.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041192**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: **LS on renumbering of 3GPP specific AVP's in 3GPP TS 23.230**
Response to:
Release: **Rel-5 & Rel-6**
Work Item: **TEI-5**

Source: **CN4**
To: **SA5**
Cc:

Contact Person:
Name: Richard Brook
Tel. Number: +44 1628 432033
E-mail Address: mailto:rbrook@nortelnetworks.com

Attachments: N4-041210

---

1. Overall Description:

Some of the RADIUS attributes used in 3GPP specifications, have a direct equivalent in 3GPP Diameter applications. In order to be possible to reuse those attributes directly in the DIAMETER specifications in form of AVP, it would be needed to use the same AVP code within the 3GPP vendor specific name space as the attribute number.

The Diameter RFC is only taking care of this backward compatibility for the IETF case, i.e. without setting the Vendor-Id, reserving the code number range from 1-255. Each vendor will manage privately AVP address space. However as Diameter was designed to be the evolution of RADIUS, and special care was taken to allow for backward compatibility, it seem reasonable that 3GPP (who uses vendor specific attributes for RADIUS and vendor specific AVPs for Diameter) manage their own address space in a similar way as IETF for backward compatibility.

CN4 has decided to renumber the AVP's assigned in TS 29.230 which prevent this backwards compatibility. Unfortunately this includes the range assigned to 32 225 which is under SA5 control.
CN4 kindly ask SA5 to amend 32.225 so it is align with 29.230
The CN4 CR to 29.230 which indicates the new AVP number range allocated to 32.225 is attached to assist in this alignment.

2. Actions:

To SA5 group.

ACTION: CN4 kindly ask SA5 to amend 32.225 so it is aligned with 29.230.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041193**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: **LS on SMS Fraud countermeasures**
Response to: **LS (**S3-040642**) from SA3**
Release: **Rel-6**
Work Item: **-**

Source: **CN4**
To: **SA3**
Cc: **T2**

Contact Person:
Name: Ulrich Wiehe
Tel. Number: +496621169139
E-mail Address: ulrich.wiehe@gksag.de

Attachments: CR 29.002 740 on SMS Fraud countermeasures (N4-040959)

---

1. Overall Description:

CN4 thank SA3 for their LS on SMS Fraud Countermeasures (S3-040642 aka N4-040914).

CN4 has assessed the proposal outlined in S3-040581. The proposal provides some level of authenticity of the SMSC address by introducing a TCAP handshake mechanism. The mechanism is already implemented in application context versions 2 and 3 for Short Message Transfer for cases where the length of the SM payload exceeds a certain limit, and it can easily be extended to be applied also for Short Messages with a shorter payload. A CR to 3GPP TS 29.002 (see attachment) would be needed to mandate the handshake mechaninsm also for short payloads at the SMS-GMSC and to reject transfer of short messages at the MSC/SGSN when Short Messages are received without handshake. A CR to 3GPP TS 23.040 is not required, however, a linked CR to 3GPP TS 33.200 is believed to be appropriate.
It must be noted that the handshake mechanism doubles the signalling load on the interfaces between SMS-GMSC and MSC / SGSN for MT short message transfer. Furthermore the mechanism requires support of application context version 2 or 3, i.e. it cannot be used with version 1.

The discussion on this was not conclusive and there was reluctance to mandate this.

2. Actions:

SA3 are asked to consider the attached CR 29.002 740 and to provide opinion on whether the solution proposed addresses the problem described in the LS S3-040642. In particular to provide guidance as to whether the proposal should be mandated or optional.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041201**
Sophia Antipolis, France. 16th to 20th August 2004.

Title:	**LS on support of the RADIUS protocol in I-WLAN**
Response to:	**LS (S2042829-N4-041172) on " Supporting RADIUS/DIAMETER Protocol at Wd Interface" from SA2**
Release:	**Rel-6**
Work Item:	**I-WLAN**
Source:	**CN4**
To:	**SA2**
Cc:	**SA5**

Contact Person:
Name: Nick Russell
Tel. Number: +44 7748 938929
E-mail Address: Nick.Russell@vodafone.com

Attachments: **None**

---

1. Overall Description:

CN4 thanks SA2 for their LS on "Supporting RADIUS/DIAMETER Protocol at Wd Interface".

CN4 gives answers to the questions that were directed to CN4 by SA2 (as paraphrased below):

Is the use of RADIUS on the Wd interface technically feasible?
CN4 has analysed a CR to 3GPP TS 29.234 (WLAN stage 3) and finds that the support of RADIUS on the Wd interface is indeed feasible.

What is the opinon of the group on the proposed change to the architecture and its complexity compared to the current architecture.
CN4 debated the issue of supporting RADIUS on the Wd interface taking into account enhancements needed to current architecture. After analysis and debate it was found that architectural impacts would be very minimal (the 3GPP AAA Proxy would now have to have the capability to proxy RADIUS messages; a process that is much simpler and therefore faster than protocol conversion) and in the end CN4 decided in favour of enhancing the Wd reference point to include RADIUS.

The Wd reference point, compared to other reference points (such as Wf, Wg, Wo etc) was considered a special case for the following reasons.

The only purpose of the Wd reference point is to proxy information from the VPLMN to the HPLMN and vice versa.

Further, it was noted that the current protocol conversion from RADIUS messages on the Wa reference point to Diameter, does *not* produce the same flow as when Diameter is used on the Wa interface. Instead a constrained or "watered down" version of the Diameter flow is produced. This is because the 3GPP AAA Proxy cannot insert missing information that would normally be present had Diameter been used on the Wa interface.

Therefore, in light of this, it was felt that allowing RADIUS on the Wd interface should be allowed.

CN4 also noted that allowing RADIUS on the Wd interface may "open the door" for proposals on the use of RADIUS on other interfaces. CN4 reccomends against this because, as far as possible, one protocol per reference point is still the preferred way. However, Wd in its role is an exception to this (due to RADIUS and Diameter having to be supported in connecting to the non-3GPP controlled entity of the WLAN AN).

In the transition from current WLAN ANs that use RADIUS to future WLAN ANs that are predicted to use Diameter, co-existence of both protocols is an unfortunate necessity for the foreseeable future.

Are any probems foreseen to arise with the interaction of the online/offline charging messages in Diameter with the user authentication and authorisation messages still in RADIUS?
CN4 believe that if there is such an issue, then this actually exists with the current architecture.

In the current architecture for the non-roaming case where the WLAN AN is using RADIUS, such an issue would be prevalent as currently it is expected that the 3GPP AAA Server (HPLMN) will have to convert the RADIUS messages received on the Wa interface to Diameter as used on the Wo and Wf reference points. CN4 notes that this is not currently explicitely stated in the WLAN stage 3 (3GPP TS 29.234).

In the current architecture for the roaming case where the WLAN AN is using RADIUS and the 3GPP AAA Proxy is translating the RADIUS messages to Diameter, these translated Diameter messages dervied from the RADIUS messages are actually a constrained version of the Diameter messages that would be conveyed from the WLAN AN when it is using Diameter. Further, when the WLAN AN network is using RADIUS and the 3GPP AAA Proxy is translating the RADIUS messages to Diameter, the 3GPP AAA Proxy conveys to the 3GPP AAA Server that the WLAN AN is using RADIUS and therefore the 3GPP AAA Server should not send any Diameter messages and/or AVPs that cannot be translated to a RADIUS message/AVP.

In the proposed new architecture for the roaming case where the WLAN AN is using RADIUS and the 3GPP AAA Proxy is simply proxying on the RADIUS messages to/from the 3GPP AAA Server from/to the WLAN AN, such functionality is analogous to the current architecture for the non-roaming case i.e. it is expected that the 3GPP AAA Server will have to convert the RADIUS messages received on the Wa interface to Diameter as used on the Wo and Wf reference points.

Given the above, CN4 believe that *should* such an issue exist, it will be prevalent whether or not the newly proposed architecture is approved.

When debating whether or not the issue does actually exist, CN4 concluded that it does not. This is because there are already standardised network nodes in the 3GPP architecture which have more than one protocol stack on them and convert the information received from one interface with one protocol stack, to be sent out on another interface with a different protocol stack. A good example of this is the GGSN where information is received on the Gn/Gp interface, which uses GTP, and which is then sent out on the Gi interface, which is RADIUS. Information such as user authentication, authorisation, and accounting/billing is already implemented in this node and is also live in operator's networks.

Are the proposed changes consistent with the IETF Diameter/RADIUS usage model?
CN4 had difficulty in understanding this question; in particular the term "IETF Diameter/RADIUS usage model". However, CN4 can see no reason why the proposed changes would not be consistent with the IETF's intended use of the Diameter and RADIUS protocols; both are currently being, and will continue to be, used for AAA procedures in WLAN interworking.

If CN4 has mis-understood the question, then CN4 invites 3GPP member companies in SA2 with these concerns to raise these with CN4 directly.

One final note on the IETF AAA WG

CN4 informs SA2 that the AAA working group in the IETF has now closed and hence, SA2 should not expect to receive an answer to their LS from this group. The only other group that *could* be asked is the RADEXT (RADIUS EXTensions) group. However, experience has shown that this group responds only to direct questions asked at the AVP level.

Instead (and as also stated above), CN4 recommends 3GPP member companies in SA2 who have concerns with whether or not IETF protocols are being mis-used, to raise this directly with CN4. CN4 can then look into this issue and liaise with the IETF, when and where appropriate, using existing mechanisms as set-up by the CN chairman (3GPP/IETF Harmonisation group).

2. Actions:

To SA2 group.

ACTION: CN4 asks SA2 to note CN4's answers to SA2's questions as stated above, and make the necessary changes to the WLAN stage 2 (3GPP TS 23.234) as appropriate to enable the RADIUS protocol to be used on the Wd interface.

CN4 also asks SA2 to note the information on IETF AAA WG and the existing communication mechanisms with raising issues with the IETF.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041202**
Sophia, France, 16 - 20 August 2004 **Agenda Item: GUP**

Title: **LS on Request for end to end example showing how the Liberty Alliance security framework fits the 3GPP GUP security requirements**
Response to: **GUP security (S3-040673).**
Release: **Rel-6**
Work Item: **GUP**

Source: **CN4**
To: **SA3**
Cc:

Contact Person:
Name: Arnaud SAHUGUET
Tel. Number: +1 908 582 6491
E-mail Address: sahuguet@lucent.com

Attachments: none

---

1. Overall Description:

CN4 thanks SA3 for the liaisons related to GUP security (S3-040673).

The current content of the "security section" of 29.240 makes reference to Liberty Alliance security framework, but in very broad terms.

The security of the Rp reference point is based on the mechanisms described in the "Liberty ID-WSF Security Mechanisms" [15] and "Liberty ID-WSF SOAP Binding" [14] specifications, and relies on:

- SSL/TLS standard mechanisms for Transport Layer Channel Protection. (other security protocols (e.g. Kerberos, IPSEC) may be used as long as they implement equivalent security measures),
- SSL/TLS for peer-to-peer authentication and X.509 v3 certificates,
- Bearer tokens or SAML assertions for message authentication.

Regarding authorization, the mentioned specifications recommend the use of the Web Services Security SAML Profile.

The specific mechanisms are further explained in the mentioned specifications, [14] and [15], and their text has preeminence to what is described here and should be considered as normative, unless explicitly indicated.

It is up to the security policy of the operator to choose which methods to apply taking into account the security domains where the client and server reside.

Among other things, it does not answer the following questions:

- Are both server and client certificates used?
- What is the topology of Certification Authorities (CAs) for these certificates?
- Are there GUP specific attributes in the X.509 v3 certificates (e.g. ESN number)?
- How do peer authentication and message authentication co-exist?
- Does the use of Web Services Security SAML profile require to introduce a new functional entity in the GUP architecture?

Moreover, the Liberty Alliance Security Framework permits to plug in any security method. In the context of GUP, some methods may not be applicable. It would be appropriate to identify and define a subset of preferred security methods for GUP.

2. Actions To SA3:

CN4 would appreciate to receive from SA3:

- an end-to-end example of the security mechanisms involved in GUP security, based on the Liberty Alliance security framework. This example would clarify – among other things – the various entities involved, the kind of messages exchanged and security methods used,
- a recommendation in terms of preferred security methods in the context of GUP.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041203**
Sophia Antipolis, France. 16th to 20th August 2004.

Title:	LS on Clarification of TMGI format
Response to:	LS (R2-041402/N4-040898) on "Reply LS on Clarification of TMGI format" from RAN2
Release:	Rel-6
Work Item:	MBMS
Source:	CN4
To:	SA1, RAN2
Cc:	SA2, CN1

Contact Person:
Name: Nick Russell
Tel. Number: +44 7748 938929
E-mail Address: Nick.Russell@vodafone.com

Attachments: None

---

1. Overall Description:

CN4 thanks RAN2 for their Liaison Statement in R2-041402/N4-040898 on "Reply LS on Clarification of TMGI format".

CN4 believes that CN4 is not the right working group to answer such a question on "Would e.g. a 2-octet MBMS service-ID not be sufficiently large to handle all realistic scenarios?" as it is believed that this is more a service requirement aspect rather than a protocol aspect; the question is more "Is 65,535 different MBMS services per operator sufficient, or is 16,777,216 more preferable?". Therefore, this question should be answered by SA1.

For the information of the groups addressed by this LS, at the protocol level in the core network, CN4 can accommodate either a 2 octet or a 3 octet service ID field in a TMGI.

2. Actions:

To SA1 group.

ACTION: CN4 asks SA1 to respond to RAN2 on whether 16,777,216 different MBMS service IDs for an operator really needed, or if 65,535 will be sufficient to meet marketing requirements, and reply directly to RAN2, copying CN4.

To RAN2 group.

ACTION: CN4 asks RAN2 to expect the answer to their question, originally posed to CN4, from SA1.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 **N4-041204**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: **LS on Evaluation of the alternatives for SMS fraud countermeasures.**

Source: **CN4**
To: **GSM-A IREG, GSM-A SG**
Cc: **SA3**

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

---

1. Overall Description:

During discussions on SMS fraud counter measures in CN4, a question regarding the desired scope of the solutions was raised. It was considered whether a solution addressing only the particular SMS fraud scenarios of 'faking' and 'spoofing' is desired, or whether in fact a greater remit is to be addressed. That remit could be to secure the SS7 network as a whole, whilst also providing a solution to the immediate SMS fraud issues.

SA3 have re-initiated the work on MAPsec within 3GPP which, when completed, would allow network operators to secure SS7 connections for all MAP messages passing between them. However, it was noted in CN4 that a similar solution would be to transport MAP over IP using SIGTRAN and to secure the IP links using IPSec. This then raised the question of the relevant timing of the two potential solutions, and hence the likelihood that MAPsec work would ultimately be deployed in networks. CN4 does not have the relevant expertise or the required operator attendance to evaluate this.

However, it would seem clear that IP and hence, SIGTRAN interconnect between operators will occur at some point in the future, whilst the work on MAPsec would also potentially lead to interconnect between operators on MAPsec secured links. It would not be good usage of 3GPP time to standardise MAPsec if IPSec interconenct will be available as a result of the widescale adoption of SIGTRAN in a similar timescale, and MAPsec would never be taken up.

2. Actions:

To GSM-A IREG and GSM-A SG group.

ACTION: CN4 asks GSM-A IREG and GSM-A SG to provide guidance to SA3 and CN4 on the expected relative timing of widescale SIGTRAN (with IPSec) interconnect between operators in comparison with MAPsec adoption and interconnect between operators.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA