3GPP TSG CN Plenary Meeting #20 **NP-030266**
4th - 6th June 2003. HÄMEENLINNA, Finland.

Source: **MCC**

Title: **All LSs sent from CN1 since TSG CN#19 meeting,- pack 2**

Agenda item: **6.1.1**

Document for: **INFORMATION**

Introduction:

This document contains **11 agreed** LSs sent from **TSG CN WG1#30**, and are forwarded to TSG CN Plenary meeting #20 for information only.

TDoc #	Status	Source	Tdoc Title	Comments
N1-030815	AGREED	Andrew H./Motorola	LS on Network Sharing Requirements for Rel-6	Reply to 578. To: SA1, Cc: SA2
N1-030817	AGREED	Inma/Nokia	Reply LS on 'Impacts on the UE of UE-Initiated Tunnelling"	Reply to 581. To: SA2, Cc: T2, SA3,
N1-030818	AGREED	Robert/Siemens	Reply LS on unciphered IMEISV transfer	Reply to 777. To: SA3
N1-030820	AGREED	Christian/ Ericsson	Reply LS on increasing the key length for GEA3	Reply to 781. To: SA3, Cc: GERAN
N1-030821	AGREED	Krisztian/ Nokia	Reply LS on media codecs and formats for Presence and Messaging	Reply to 783. To: SA4, Cc: SA2
N1-030836	AGREED	Robert/Siemens	LS on Support of additional LLC SAPIs	Reply to 813. To: SA2, Cc: GERAN
N1-030877	AGREED	Kevan/3	Reply LS on RAN WG2 terminology and impacts on CN WG1 specifications (PLMN selection)	Reply to 865. To: RAN2
N1-030896	AGREED	Nokia / Georg	LS on transport of unknown SIP signaling elements	Linked to 895. To: SA2, SA3, SA5
N1-030918	AGREED	Kevan/3	LS on Security Association Lifetimes	Linked to 645. To: SA3, Revised from 888.
N1-030933	AGREED	Peter/Siemens	LS on security solutions for the Mt reference point	Reply to 780. To: SA3, Cc: SA2 Revised from 819
N1-030944	AGREED	Atle/Ericsson	Reply LS on R99 and later emergency calls when attached to data only network	Reply to 579. To: SA1, SA2, Cc: GERAN2, RAN2, Revised from 816 and 932

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030817***
San Diego, California, USA, 19 – 23 May 2003

Title: Reply LS on 'Impacts on the UE of UE-Initiated Tunnelling"
Response to: LS (N1-030581/S2-031569) on 'Impacts on the UE of UE-Initiated Tunnelling" from SA2
Release: Rel6
Work Item: WLAN-3GPP WI

Source: CN1
To: SA2
Cc: T2, SA3

Contact Person:
Name: **Inma Carrion**
Tel. Number: +358503806481
E-mail Address: inmaculada.carrion-rodrigo@nokia.com

---

1. Overall Description:

CN1 would like to thank SA2 for their liaison "Impact on the UE of UE-Initiated Tunnelling". In this LS (N1-030581/S2-031569) CN1 was requested to evaluate the UE-Initiated tunnel and to check whether tunnel security options may impact the UE.

CN1 understands that the UE-Initiated tunnel is a feature in WLAN UEs, needed to support scenario 3 type of service for WLAN-3GPP IW. It was discussed that this feature requires a client in the terminal, such as VPN client.

At this point CN1 could not foresee any specific impact that would not allow Rel6 WLAN terminals to support UE-Initiated tunnel.

There were some discussions regarding the security in UE-Initiated tunnels using e.g. IPSec. However, it was noted that this discussion should take place in SA3.

CN1 would like to take the chance to inform SA2 that it has just started the WLAN related Stage 3 work. It is focussing in the WLAN authentication between the UE and 3GPP AAA Server using EAP/AKA and EAP/SIM procedures.

2. Actions:

To SA2 group.

ACTION: None.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	China

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030815***
San Diego, California, USA, 19 – 23 May 2003

Agenda item: 9

Document for: LS Out

Title: ~~Draft~~ **LS on Network Sharing Requirements for Rel-6**
Release: Rel-6
Work Item: Network Sharing

Source: **CN1**
To: SA1
Cc: SA2

Contact Person:
Name: Andrew Howell
Tel. Number: +44 1452 623967
E-mail Address: **andrew.howell@motorola.com**

Attachments: None

---

1. Overall Description:

CN1 thanks SA1 for their liaison statement on Network Sharing (TDoc S1-030533).

CN1 has noted the 22.011 CR, covering changes to the PLMN selection requirements, and can confirm that the CR is seen as sufficiently clear to allow CN1 to continue with the Stage 3 work, once the necessary Stage 2 information is received from SA2.

CN1 has discussed the following working assumptions:

- Multiple PLMN (MCC + MNC) information will be broadcast via the shared AN cells.
- Cell selection and re-selection ~~and LA~~ concepts are to be kept as they are, for as long as possible.
- LA / RA concepts are to be kept as they are, for as long as possible.
- All UEs accessing any of the PLMNs via the shared AN should see the same LA / RA identities and borders to avoid problems with old mobiles, cell planning interactions with LA, and National roaming and regional provision concepts.
- There will be a single Network Mode of Operation (NMO) for all UEs accessing the shared AN area.
- Legacy mobiles must be supported.

Based on the above working assumptions it appears that ~~All these seem to indicate that~~ only multiple MCC + MNC information needs to be added to the broadcast ~~and the rest of the~~ system information. All other broadcast system information~~-~~ needs to be kept as it is.~~, as long as possible.~~

2. Actions:

To SA1 group.

ACTION:

CN1 would like to ask SA1 to confirm that the working assumptions meet their requirements.

3. Date of Next TSG-CN WG1 Meetings:

CN1#31	25 – 29 August 2003,	Sophia Antipolis, hosted by ETSI
CN1#32	27 – 31 October 2003,	China, Japanese Friends of 3GPP and Ericsson China

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030818***
San Diego, California, USA, 19 – 23 May 2003

Title: Reply LS on unciphered IMEISV transfer
Response to: LS (S3-030294/N1-030777)
Release: ---
Work Item: Early UE

Source: CN1
To: SA3

Contact Person:
Name: Robert Zaus
Tel. Number: +49 89 636 75206
E-mail Address: robert.zaus@siemens.com

Attachments: ---

---

1. Overall Description:

CN1 would like to thank SA3 for their LS on unciphered IMEISV transfer.

CN1 has checked TS 24.008 and confirms that the stage 3 specification does not include any timing restrictions for the MSC/VLR, SGSN, or UE on the handling of an IMEISV request. I.e. an identity request for the IMEISV (or IMEI) before activation of the security mode control procedure is not forbidden, and it is not forbidden for the UE to reply to such a request.

2. Actions:

---

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	???, ???

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030820***
San Diego, California, USA, 19 – 23 May 2003

Title: **Reply LS on increasing the key length for GEA3**
Response to: LS (S3-030308) on increasing the key length for GEA3

Source: CN1
To: SA3
Cc: GERAN

Contact Person:
Name: Christian Herrero, Ericsson
Tel. Number: +46 46 231812
E-mail Address: Christian.Herrero@emp.ericsson.se

Attachments: None.

---

1. Overall Description:

CN1 thanks SA3 for their LS in S3-030308 on the increase of the key length for GEA3.

CN1 would like to inform SA3 that the current definition of the MS Network Capability information element -sub clause 10.5.5.12 in TS 24.008- already contains a code point for GEA4 that was defined long time ago. Hence, code point GEA4 is a suitable indication for support of the GEA4 algorithm in the mobile station.

2. Actions:

To SA3 group.

CN1 kindly recommends SA3 to consider this information and take it into account when making a final decision on the increase of the key length for GEA3.

3. Date of Next TSG-CN WG1 Meetings:

TSG-CN WG1 Meeting #31	25 – 29 August 2003	Sophia Antipolis, France.
TSG-CN WG1 Meeting #32	27 – 31 October 2003	TBD.

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030821***
San Diego, California, USA, 19 – 23 May 2003

Title: **Reply LS on media codecs and formats for Presence and Messaging**
Response to: LS (S4-030418, N1-030783) on Reply LS on media codecs and formats for Presence and Messaging from SA WG4
Release: 6
Work Item: PRESNC

Source: CN WG1
To: SA WG4
Cc: SA WG2

Contact Person:
Name: Krisztian Kiss
Tel. Number: +358504835363
E-mail Address: krisztian.kiss@nokia.com

Attachments: draft-lonnfors-simple-binpidf-01, draft-ietf-sip-congestsafe-01

---

1. Overall Description:

CN WG1 would like to inform SA WG4 that CN WG1 has adopted draft-lonnfors-simple-binpidf-01 (and its future revisions) on referencing external objects from the Presence Information Data Format. The draft is referenced from TR 24.841, as well as it is part of the normative Rel-6 dependency list CN WG1 produced.

Furthermore, CN WG1 plans to adopt draft-ietf-sip-congestsafe-01 (and its future revisions) for the Rel-6 IM CN Subsystem in order to prohibit the risk of network congestion when transmitting large SIP messages over UDP. The Internet-Draft is part of the normative Rel-6 dependency list, its final adoption depends on the progress of the draft in the SIP WG.

2. Actions:

To SA WG4 group.

ACTION: CN WG1 asks SA WG4 to take into account the above discussion when progressing with the codec and format definition work for presence and messaging.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	China

SIP -- Session Initiation Protocol
Working Group
Internet-Draft
Expires: August 13, 2003

D. Willis
B. Campbell
dynamicsoft Inc.

Feb 12, 2003

Session Initiation Protocol Extension to Assure Congestion Safety

draft-ietf-sip-congestsafe-01

Status of this Memo

Copyright Notice

Abstract

The Session Initiation Protocol allows the use of UDP for transport

of SIP messages. The use of UDP inherently risks network congestion problems, as UDP itself does not define congestion prevention, avoidance, detection, or correction mechanisms. This problem is aggravated by large SIP messages which fragment at the UDP level. Transport protocols in SIP are also negotiated on a per-hop basis, at the SIP level, so SIP proxies may convert from TCP to UDP and so forth. This document defines what it means for SIP nodes to be congestion safe and specifies an extension by which a SIP User Agent may require that its requests are treated in a congestion safe manner.

Table of Contents

1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Background

The Session Initiation Protocol RFC 3261 [4] provides application support over multiple transport protocols, including UDP and TCP. Transport negotiation is not "end to end" with SIP. Instead, each SIP hop individually determines which transport to use. For example, a User Agent (UA) may use TCP to talk to a proxy, that proxy my use UDP to talk to another proxy, and that second proxy may use SCTP to talk to a destination UA.

UDP has inherent issues with congestion management. The protocol has not explicit mechanisms for avoiding, detecting, or adapting to network congestion. SIP attempts to deal with this in two ways:

1. Retransmission timers with exponential back offs.
2. Attempting to limit the size of transmissions over UDP to reduce the effects of fragmentation.

This would appear to be an incomplete solution. One solution might be to deprecate UDP entirely for SIP. However, there is a large installed base using UDP, and there are legitimately places where UDP appears to be quite useful such as tiny mobile phones and in extremely high-volume proxies connecting over dedicated networks.

As an alternative, this draft:

1. Defines what it means for a SIP node to be "congestion-safe".
2. Defines a mechanism whereby a congestion-safe UA may require that any proxy processing its requests be congestion safe.
3. Defines a mechanism whereby a proxy may reject a request that it would be forced to fragment, and in so doing inform the originating UA of relevant sizing parameters.

4. Defines a mechanism whereby a server may reject requests that would result in responses that might not be transmitted congestion-safely if the request itself was not received in a congestion-safe manner.

3. Definition of Congestion Safety for SIP

A SIP node can be considered "congestion safe" if it never emits a request or response in a manner not known to be congestion safe.

Requests may be considered congestion-safe if any one of the following criteria is met:

1. The transport toward the next SIP hop is TCP, SCTP, or other transport providing congestion control and the next hop is known to be either a UA or a congestion-safe proxy.
2. The transport toward the next hop is UDP, the next hop is known to be a UA or congestion-safe proxy, and the network between the two is known to support congestion management at a lower layer. Note that this is an uncomoon case in typical Internet applications.
3. If the only available transport toward the next hop is UDP and the next hop is known to be a UA or congestion-safe proxy, the request MAY be transmitted over UDP or rejected by local policy. If the request is transmitted over UDP, the procedures described under the heading "Responsible use of SIP over UDP" in this document MUST be followed.

Responses may be considered congestion-safe if any one of the following criteria is met:

1. The request was congestion-safe, as defined above.
2. The response is no larger than the request.

The preceding uses the phrase "the next hop is known to be either a UA or a congestion-safe proxy." Such knowledge may be derived either through administrative configuration or through use of the Proxy-Require mechanism defined herein under the heading "Assuring Transitive Congestion Safety with Proxy-Require".

4. Assuring Transitive Congestion Safety with Proxy-Require

SIP provides a mechanism whereby a user agent making a request can be assured that any proxy servicing that request support a specific extension or set of behavior. To do so, the user agent includes a "Proxy-Require" header field with a value indicating a tag for the specific extension or behavior required. There is an IANA registration process for these tags. As per [4], proxies not recognizing a specific tag or unwilling to support the associated behavior reject a request referencing that tag with a 420 response,

which has the semantic "Unsupported".

We herein define a tag value of "congestion-safe". A proxy forwarding a request containing a Proxy-Require with this tag value MUST manifest the property of congestion-safety as defined by this document.

5. Responsible use of SIP over UDP

The fundamental problem with UDP is that it provides no feedback mechanism to allow a sender to pace its transmissions against the real performance of the network. While this tends to have no

significant effect on extremely low-volume sender-receiver pairs, the impact of high-volume relationships on the network can be severe. Consider the following scenario, wherein the traffic between multiple UAs is funnelled through a single proxy-proxy relationship.

Example of large-fan out/fan-in likely to encounter congestion:

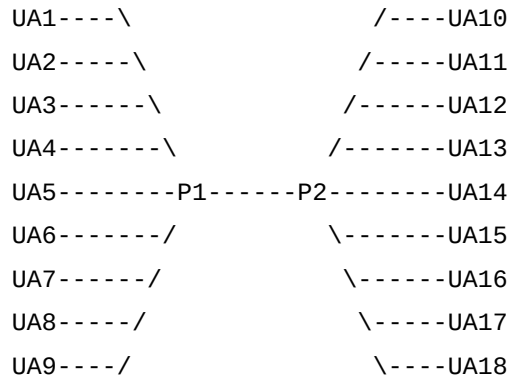

Figure 1

In this scenario, any requests from UA(1..9) to UA(10..18) traverse the proxy-proxy link P1&lt-->P2. Assuming current SIP practices, if this link is UDP and every UA emits a request simultaneously, each proxy will insert nine (one for each UA) requests, resulting in eighteen simultaneous requests on the P1&lt-->P2 link. Each request may require retransmissions, and large requests may require fragmentation to fit the link MTU -- at the worst case, producing more than one hundred packets per request, or approximately 2,000 simultaneously expressed packets in this scenario. If the capacity of link P1&lt-->P2 is inadequate to deliver these messages within the SIP retransmission window, the originating UAs (or the proxies, if acting in transaction-stateful mode) generate retransmissions, further compounding the problem into a "retransmission storm". Real-world scenarios may scale far more seriously. It is not

unreasonable to assume that there may be tens of thousands of UAs on each side of the network.

Clearly the best thing to do is to use a more sophisticated transport protocol (TCP, SCTP, etc.) between P1 and P2, and between each UA and its associated proxy. If this is not feasible, it may be necessary to fall back to UDP.

It should be noted that the fundamental problem not just between UAs and proxies, but whenever there is a high fan-out or fan-in ratio. If in the above example, each UA were behind a "residential proxy", the problem would occur in similar fashion.

One might propose that SIP ALWAYS use a congestion-controlled transport to talk to proxies, and only fall back to UDP when the next hop is a UA. The primary problem with this approach is that in general, a SIP node does not and cannot know whether the next node is a UA or a proxy -- it is this ability to "insert" proxies into a sequence that provides much of the flexibility of SIP. A secondary problem is that even if the next hop is a UA, some UAs are sufficienty high volume, and some links sufficiently narrow, that congestion might still result from the incautious use of UDP.

5.1 Requirements For Use of SIP Over UDP

The previously described problems with the general use of SIP over UDP lead to the following two requirements for the use of UDP as a transport protocol for SIP:

1. Large messages MUST NOT be transmitted over UDP. The SIP specification provides basic guidance for UAs. Congestion-safe proxies MUST follow the procedures described below under the heading "Proxy Rejects Request That Would Require UDP Fragmentation." UAs MAY also make use of the MTU feedback techniques in that section.
2. Nodes sending requests over UDP MUST pace those requests as described under the heading "Pacing SIP requests over UDP."

Response messages SHOULD be constrained to be smaller than the MTUs established for requests by the preceding mechanisms, and systems implementors should remain aware that SIP provides limited support for managing response sizes. Further experience may indicate a need for further control over response handling.

5.2 Pacing SIP Requests Over UDP

One simple way to describe the congestion problem is that UDP lets us send packets without knowing whether those packets are arriving. The simplest approach to dealing with this at the application level is to send a request, then wait for some sort of response indicating that

the request was received before sending anything else. This produces an effect described by some as "ping-ponging" -- traffic bounces back and forth between two nodes like a ping-pong ball or tennis ball in a match. Since there's only one ball in play between any two players at any given time, most of the potential for congestion cascades is eliminated.

This pacing or serialization approach has the side-effect of significantly reducing the maximum throughput, as transmission occurs in only one direction at a time and there is at least a 2xRTT delay between transmissions. More sophisticated algorithms such as those in TCP and SCTP have been developed to address this, and it would be

inappropriate to duplicate that work here. Consequently, if greater efficiency is required than that provided by this simple approach, implementors should use TCP, SCTP, or another such protocol. But if one absolutely must use UDP, this approach works, and is reasonably efficient in the most likely application of "edge proxy" to UA and other proxies with large fan-outs to individual low-volume nodes.

SIP has two sorts of request transactions: "invite" and "non-invite" tranactions. Invite transaction use a three way sequence of "request, response, acknowledgement" and may include a "provisional response" between the request and response steps. Non-invite transactions use a two-way "request, response" sequence, and may also have a provisional response although that behavior has been deprecated.

Congestion-safe use of SIP over UDP requires waiting for some sort of response to a request (or a timeout, which has backoff properties) before sending another request to that same destination. A congestion-safe SIP node (UA or proxy) MUST NOT send a request to a given next-hop if there is an existing request to that destination which has not received some sort of response. The existing transaction MUST either receive a response (final or provisional) or time-out before a new request can be made to that next-hop.

This effectively requires congestion-safe proxies to act in a transaction-stateful manner on a per-next-hop destination basis, at least to the extent of tracking whether some sort of request is pending to each next-hop and correlating provisional and final responses to that request.

Some may argue that this puts an excessive burden onto the SIP node, and that implementations that are "congestion-safe" per this specification will have reduced performance when used with UDP over a shared or public network. We counter that congestion-safe transport protocols are readily available, and that network users which insist on using unsafe transports (such as UDP) MUST be responsible for

assuring that they do not impede the function of other users of the network, even at the expense of reducing their own efficiency. It is simply irresponsible to "blast away" at the network without regard for congestion or its impact on other users of the network.

5.3 Proxy Rejects Request That Would Require UDP Fragmentation

A proxy may be faced with a request to deliver a large message using UDP as a transport. Fragmentation of such messages is problematic in several ways. Loss of any fragment requires time-out and retransmission of the message. The fragments are commonly transmitted out the interface at local interface (usually LAN) rates,

without awareness of intervening network conditions. For these reason, we believe it in general a bad practice to send large requests over UDP.

While the actual MTU of a link may not be known, common practice seems to indicate that the local interface MTU is likely to be a reasonable approximation. Where the actual path MTU is known, that value should be used instead.

When a congestion-safe SIP proxy processing a request determines that the next hop is reached via UDP, and that the request is larger than the effective MTU toward that hop and would consequently be fragmented, the proxy MUST reject that request with a 513 response.

The base SIP specification provides minimal guidance on dealing with oversized requests. There is an error response code, 513, with the semantic "request too large" that seems applicable. However, SIP provides no guidance on how to indicate what size might be allowed. We define here two extension header fields that may be used in a 513 response to indicate by the rejecting proxy the size of message allowed by that proxy. The extension header field "Proxy-Max-Size" may be used to indicate the largest allowable request to the originating UA. The extension header field "Proxy-Seen-Size" may be used to indicate the size of the rejected request as calculated by the rejecting proxy. In both cases, the size value used indicates the SIP message size, which does not include IP or transport protocol overhead.

A congestion-safe SIP proxy which rejects a request based on size SHOULD include a "Proxy-Max-Size" header field with a value indicating the largest size message allowed by this proxy on this link. If a Proxy-Max-Size header field is sent, the proxy MUST also include a "Proxy-Seen-Size" header indicating the size of the request as seen at this proxy.

A UA receiving a 513 response has the options of giving up, trying a

smaller request, or trying a different set of proxies. Should it choose to try a smaller request, it may estimate the size of the largest message that can be sent by taking the original request size, subtracting it from the value of the Proxy-Seen-Size header field, and subtracting that result from the value of the Proxy-max-Size header field. Note that a UA SHOULD NOT repeatedly downsize and retry a request. This technique is not an adequate replacement for TCP's Path MTU Discovery. Any request that has been rejected more than once with a 513 SHOULD either be abandoned or re-issued over congestion-safe channels.

5.4 Server Rejects Request Because Response Could Not Be Sent Safely

A server receiving a SIP request generates a resposne to that request. Delivery of this response may raise issues of congestion-safety. Because SIP requires that responses traverse exactly the reverse of the route taken by the request (recorded in the Via: header fields values), the server has no options about routing the response. If the request was delivered in a congestion-safe manner, it can be safely assumed that the response will also be returned in a congestion-safe manner, as it must traverse exactly this recorded route. However, if the request was NOT received in a congestion-safe manner, the server cannot negotiate a congestion-safe path for the response, as the response must follow the path of the request.

If the size of the generated response is less than the size of the received request, it may be reasonably assumed that since the request arrived intact, a response of equal or smaller size is likely to traverse the reverse of that path succesfully. However, no such assumptions can be made about responses that are larger than the corresponding request.

When a congestion-safe server generates a response to a request that is larger than the request and that request was not received over a congestion-safe channel, it cannot be assumed that the response can be safely transmitted. An unsafe response cannot be transmitted by a congestion-safe server. Instead the server MUST reject the request and return an error response using response code 514, which has the semantic of "Response Could Not Be Sent Safely".

A UA receiving a 514 response to a request may either retry the request in a congestion-safe manner or abandon the request.

6. Syntax of Extensions and Changes to SIP Specifications

The syntax for the Proxy-Max-Size header field is:

Proxy-Max-Size = "Proxy-Max-Size" HCOLON 1*DIGIT

The syntax for the Proxy-Seen-Size header field is:

Proxy-Seen-Size = "Proxy-Seen-Size" HCOLON 1*DIGIT

7. IANA Considerations

This document defines the SIP extension header fields "Proxy-Max-Size" and "Proxy-Seen-Size" ", which IANA will add to the registry of SIP header fields defined in [4].

This document also defines the SIP option tag "congestion-safe" which IANA will add to the registry of SIP option tags defined in [4].

This document also defines the SIP response code 514, with the semantic "Response Cannot Be Sent Safely" which IANA will add to the registry of SIP response codes defined in [4] in the section for 5xx clase response codes.

The following is the registration for the Proxy-Max-Size header field:

RFC Number: RFCXXXX [Note to IANA: Fill in with the RFC number of this specification.]

Header Field Name: Proxy-Max-Size

Compact Form: none

The following is the registration for the Proxy-Seen-Size header field:

RFC Number: RFCXXXX [Note to IANA: Fill in with the RFC number of this specification.]

Header Field Name: Proxy-Seen-Size

Compact Form: none

The following is the registration for the congestion-safe option tag:

RFC Number: RFCXXXX [Note to IANA: Fill in with the RFC number of this specification.]

Option Tag: congestion-safe

The following is the registration for the SIP response code 514:

RFC Number: RFCXXXX [Note to IANA: Fill in with the RFC number of this specification.]

Response Code: 514 Response Cannot Be Sent Safely

8. Acknowledgements

Robert Sparks and Jonathan Rosenberg argued with us vociferously over this topic and contributed substantial insight.

Normative References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Postel, J. and J. Reynolds, "Instructions to RFC Authors", RFC 2223, October 1997.

[4] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[5] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J. and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", BCP 67, RFC 3427, December 2002.

Authors' Addresses

Dean Willis
dynamicsoft Inc.
5100 Tennyson Parkway
Suite 1200
Plano, TX 75028
US

Phone: +1 972 473 5455
EMail: dean.willis@softarmor.com
URI: http://www.dynamicsoft.com/

Ben Campbell
dynamicsoft Inc.

5100 Tennyson Parkway
Suite 1200
Plano, TX 75028
US

Phone: +1 972 473 5452
EMail: bcampbell@dynamicsoft.com
URI: http://www.dynamicsoft.com/

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

SIMPLE WG
Internet-Draft
Expires: November 5, 2003

M. Lonnfors
Nokia Research Center
E. Leppanen
H. Khartabil
Nokia

May 7, 2003

BINPIDF - External Object Extension to Presence Information Data Format

draft-lonnfors-simple-binpidf-01

Status of this Memo

Copyright Notice

Abstract

This memo specifies a methodology whereby external content to a presence information document can be referenced in XML encoded presence information document (PIDF). The external content can be either transferred directly in the payload of messages or indirectly as an HTTP reference. The external part might contain binary data such as images.

Table of Contents

1. Introduction

The Presence Information Data Format (PIDF) is described in [2]. It defines a generic XML encoded format to express a presentity's presence information. However, it does not specify any mechanism how external objects, e.g. pictures, as a part of presence information can be represented in such XML documents.

The Content Indirection document [4] provides an extension to the URL MIME External-Body Access-Type [8] to allow any MIME part in a SIP message to be referred indirectly via a URL. In addition there is a need to specify an extension to PIDF in order to use the Content Indirection mechanism for the Presence in a way that the XML encoded presence information is carried directly in MIME message while external objects are referenced indirectly.

Using the SIP Events [5] as transport for PIDF documents it is equally feasible to deliver the external objects in the payload of a SIP message, namely SIP NOTIFY. The MIME Multipart/Related content type [6] provides a tool for placing a reference to an external content as a MIME multipart. An extension to PIDF is needed for referencing the multiparts from a PIDF formatted presence information document. A similar kind of approach of utilizing the MIME Multipart/ Related with HTML can be found in [7].

2. Conventions

In this document, the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 [1] and indicate requirement levels for compliant implementations.

3. Overview of Methodology

This section provides an overview for having references to the external objects (direct and indirect content) in presence

information.

The external object can be embedded as one part of a multipart payload of a MIME message, can be stored at an external location where the multipart payload includes a URL to external object using Content Indirection [4], or the PIDF XML part can directly contain a URL link to the content. The MIME Multipart/Related content type [6] is used for direct delivery of the external object.

The presence information data format is extended with an object link (ObjLink) XML element. Each separate external content has its own ObjLink value within presence information. The value of the ObjLink

is URL (see more information about the syntax of URL from [9]). The value might be either the Content ID of the external object part in the multipart payload or a URL to the location of the external content. The application processing the PIDF document is able to discover the location of the content from the scheme of the URL (see more information about the reserved scheme names from [9] and [10]). The 'cid:' scheme [10] refers to a specific body part of a message.

4. BINPIDF Elements

4.1 Namespace

The namespace declaration to the PIDF extension specified in this document is 'urn:ietf:params:xml:ns:pidf-ext-cont'.

4.2 'ObjLink' Element

The 'ObjLink' XML element contains a URL reference [9] to the external object. The scheme of the URL specifies how the value of the ObjLink element is processed. The value of the ObjLink might correspond to the Content ID [10] parameter of the multipart made according to MIME Multipart/Related content type [6], or to the 'external' location of the content.

The ObjLink element MAY have a ContentType attribute. The ContentType should be used when the URL references directly to an external location. The value of the attribute describes the content (see description of entity headers from [11]).

5. How To Utilize this Specification

This chapter describes how the payload of a SIP message is composed when there is a need to convey external objects to XML encoded presence information document between the client and presence server.

The following methods for delivering the external object are

explained later in their own subchapters: a direct link to the external content within a PIDF based XML document and a reference to a multipart having either the content of the external object embedded or a URL (and other information) to an external location where the content is stored.

5.1 Direct Link to External Content

The ObjLink XML element is included in PIDF to point to the location where the external content is stored. The used content type in the SIP message is one of the normal content type(s) of presence service.

5.2 Reference to Multipart where External Object is Embedded

The content type of the SIP message and the multiparts of the payload are composed according to [6] (MIME Multipart/Related). The XML encoded presence information in PIDF is the 'root' of the body part. The ObjLink XML element is used within presence information in PIDF to reference to the multipart where the content of the external object is found.

5.3 Reference to Multipart where Link and Another Information about the External Object is Found

The content type of the SIP message and the multiparts of the payload are composed according to [6] (MIME Multipart/Related). The XML encoded presence information in PIDF is the 'root' of the body part. The ObjLink XML element is used within presence information in PIDF to reference the part in the multipart payload where the additional information (e.g., URL) of the external object is found. The multipart of the external object is composed according to [4].

6. Examples

6.1 Binary Objects both Directly Embedded and Indirectly Referenced in Multiparts

Presence information subscription from client to server:

```
SUBSCRIBE sip:john@pres.example.com SIP/2.0
Via: SIP/2.0/TCP xxxxx;branch=z9hG4bKwYb6QREiCL
Max-Forwards: 70
To: <sip:john@pres.example.com>
From: <sip:adam@example.com>;tag=ie4hbb8t
Call-ID: cdB34qLToC@terminal.example.com
CSeq: 322723822 SUBSCRIBE
Contact: xxxx
Event: presence
```

```
      Expires: 7200
      Accept: application/cpim-pidf+xml
      Accept: multipart/related
      Accept: message/external-body, text/html, text/plain, image/*
      Content-Length: 0

      (200 OK are omitted)
```

The NOTIFY looks like:

```
      NOTIFY sip:terminal.example.com SIP/2.0
      Via: SIP/2.0/TCP pres.example.com;branch=z9hG4bKMgRenTETmm
```

```
Max-Forwards: 70
From: <sip:john@pres.example.com>;tag=zpNctbZq
To: <sip:adam@example.com>;tag=ie4hbb8t
Call-ID: cdB34qLToC@terminal.example.com
CSeq: 997935768 NOTIFY
Contact: <sip:pres.example.com>
Event: presence
Subscription-State: active;expires=7200
Content-Type: multipart/related;type="application/cpim-pidf+xml";
    start="<nXYxAE@pres.example.com>";boundary="50UBfW7LSCVLtggUPe5z"
Content-Length: xxx

--50UBfW7LSCVLtggUPe5z
Content-Transfer-Encoding: 8bit
Content-ID: <nXYxAE@pres.example.com>
Content-Type: application/cpim-pidf+xml;charset="UTF-8"

<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:cpim-pidf"
       xmlns:obj="urn:ietf:params:xml:ns:pidf-ext-cont"
       entity="sip:john@pres.example.com">

    <tuple id="432sd">
       <status>
         <basic>open</basic>
       </status>
       <contact>sip:john@im.example.com</contact>
          <note>At home</note>
          <obj:ObjLink>cid:own_photo@example.com</obj:ObjLink>
          <obj:ObjLink>cid:image1@example.com</obj:ObjLink>
     </tuple>
   </presence>

 --50UBfW7LSCVLtggUPe5z
  Content-Type: image/jpeg
  Content-ID: <own_photo@example.com>
```

```
Content-Transfer-Encoding: binary
Content-Description: Own photo

(encoded jpeg image)

--50UBfW7LSCVLtggUPe5z
Content-Type: message/external-body
Content-ID: <image1@example.com>
Content-Disposition: render
Content-Description: Group photo

Content-Type: message/external-body;
```

```
                    access-type="URL";
                    expiration="Mon, 24 June 200x 09:00:00 GMT";
                    URL="http://www.ex.com/company_party/image1.png"
                    size=234422

       --50UBfW7LSCVLtggUPe5z
```

6.2 External Content Reference in Presence Information without MIME Multipart Definition

Presence information subscription from client to server:

```
SUBSCRIBE sip:john@pres.example.com SIP/2.0
Via: SIP/2.0/TCP xxxxx;branch=z9hG4bKwYb6QREiCL
Max-Forwards: 70
To: <sip:john@pres.example.com>
From: <sip:adam@example.com>;tag=ie4hbb8t
Call-ID: cdB34qLToC@terminal.example.com
CSeq: 322723822 SUBSCRIBE
Contact: xxxx
Event: presence
Expires: 7200
Accept: application/cpim-pidf+xml
Accept: image/*
Content-Length: 0
```

Notification having a link to the picture:

```
NOTIFY sip:terminal.example.com SIP/2.0
Via: SIP/2.0/TCP pres.example.com;branch=z9hG4bKMgRenTETmm
Max-Forwards: 70
From: <sip:john@pres.example.com>;tag=zpNctbZq
To: <sip:adam@example.com>;tag=ie4hbb8t
Call-ID: cdB34qLToC@terminal.example.com
CSeq: 997935768 NOTIFY
```

```
Contact: <sip:pres.example.com>
Event: presence
Subscription-State: active;expires=7200
Content-Type: application/cpim-pidf+xml
Content-Length: xxx

   <?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:cpim-pidf"
       xmlns:obj="urn:ietf:params:xml:ns:pidf-ext-cont"
       entity="sip:john@pres.example.com">

    <tuple id="432sd">
```

```
            <status>
              <basic>open</basic>
            </status>
            <contact>sip:john@im.example.com</contact>
            <note>At home</note>
            <obj:ObjLink
ContentType="image/jpeg">http://www.example.com/own_photo.jpg</obj:ObjLink>
          </tuple>
        </presence>
```

7. XML Schema Definition

```
      <?xml version="1.0" encoding="UTF-8"?>
      <xs:schema targetNamespace="urn:ietf:params:xml:ns:pidf-ext-cont"
                  xmlns:xs=http://www.w3.org/2001/XMLSchema
                  elementFormDetault="qualified"
                  attributeFormDefault="unqualified">
            <xs:element name="ObjLink">
                <xs:complexType>
                      <xs:simpleContent>
                          <xs:extension base="xs:anyURI">
                            <xs:attribute name="ContentType" type=xs:string
use="optional"/>
                        </xs:extension>
                    </xs:simpleContent>
                </xs:complexType>
            <xs:/element>
      </xs:schema>
```

8. Security Considerations

All security concideration defined in [5] and [4] apply this document.

9. Acknowledgements

The authors would like to thank Aki Niemi for his valuable input.

10. Changes from the Version 00

- Two XML extension elements (ExtLink and CId) were combined together and named as ObjLink.
- Optional ContentType attribute was added to the ObjLink element.
- References to the syntax of URL and pre-defined scemes were added.
- Content type negotiation related texts were removed from the

Section 5.

- Some editorial corrections.

References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Sugano, H., "CPIM Presence Information Data Format", draft-ietf-impp-cpim-pidf-07.txt, December 2002.

[3] Campbell, B., "SIMPLE Presence Publication Mechanism", draft-olson-simple-publish-02.txt, February 2003.

[4] Olson, S., "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", draft-ietf-sip-content-indirect-mech-01, February 2003.

[5] Rosenberg, J., "Session Initiation Protocol (SIP) Extensions for Presence", draft-ietf-simple-presence-10.txt, January 2003.

[6] Levinson, E., "The MIME Multipart/Related Content Type", RFC 2387, August 1998.

[7] Palme, J., "MIME Encapsulation of Aggregate Documents", RFC 2557, March 1999.

[8] Freed, N., "Definition of the URL MIME External-Body Access-Type", RFC 2017, October 1996.

[9] Berners-Lee, T., "Uniform Resource Locators (URL)", RFC 1738, December 1994.

[10] Levinson, E., "Content-ID and Message-ID Uniform Resource

Locators", RFC 2392, August 1998.

[11] Freed, N., "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

Authors' Addresses

Mikko Lonnfors
Nokia Research Center
Itamerenkatu 00180
Helsinki
Finland

Phone: + 358 50 4836402
EMail: mikko.lonnfors@nokia.com

Eva Leppanen
Nokia
P.O BOX 785
Tampere
Finland

Phone: +358 7180 77066
EMail: eva-maria.leppanen@nokia.com

Hisham Khartabil
Nokia
P.O. Box 321
Helsinki
Finland

Phone: +358 7180 76161
EMail: hisham.khartabil@nokia.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030836***
San Diego, California, USA, 19 – 23 May 2003

Title: LS on Support of additional LLC SAPIs
Response to: LS (S2-032177/N1-030813) on < Mapping of NSAPIs onto LLC SAPIs > from SA2
Release: Release 6
Work Item: TEI-6
Source: CN1
To: SA2
Cc: GERAN

Contact Person:
Name: Robert Zaus
Tel. Number: +49 89 636 75206
E-mail Address: robert.zaus@siemens.com

Attachments: ---

---

1. Overall Description:

CN1 would like to thank SA2 for their LS on Mapping of NSAPIs onto LLC SAPIs.

SA2 have asked CN1 to study whether more LLC SAPIs could be made available for a UE and to extend the number of LLC SAPIs if feasible.

CN1 have briefly discussed the issue and can provide the following preliminary answer:

- Currently, in the *LLC service access point identifier* IE in TS 24.008 only 4 LLC SAPI values have been defined for GPRS data transfer. One additional codepoint ("0000") is used to indicate "LLC SAPI not assigned".

- All the remaining code points are defined as "reserved". Therefore, it is not possible to use these code points in the existing *LLC service access point identifier* IE for extension, since an old SGSN implementation would have to reject a message containing a reserved value in a mandatory IE. However, a new IE or an indication of support of new LLC SAPIs from the receiving entity could be used as a workaround.

CN1 needs to study these possible solutions in more detail and will inform SA2 and GERAN when progress has been made on the issue.

2. Actions:

---

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	???, ???

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030877*
San Diego, California, USA, 19 – 23 May 2003

Title: **Reply** LS on **RAN WG2 terminology and impacts on CN WG1 specifications (PLMN selection)**
Response to: LS (N1-030865 / R2-031368) on **RAN WG2 terminology and impacts on CN WG1 specifications (PLMN selection)**
Release: Release 99
Work Item:

Source: CN1
To: RAN2
Cc:

Contact Person:
Name: Kevan Hobbis
Tel. Number: + 44 7782 325252
E-mail Address: kevan.hobbis@three.co.uk

Attachments:

---

1. Overall Description:

CN1 thanks RAN2 for their liaison on terminology. Discussion in CN1 has concluded that the issues raised are not purely down to terminology differences. Although it is clear that there is a discrepancy in the understanding of the term 'dedicated channel' between CN1 and RAN2.

CN1 notes that TS23.122 defines the procedures and conditions for PLMN selection in the Non-Access Stratum. CN1 has a concern that a simple alignment of terminology may result in a partial merging of the NAS and AS layers, e.g. MM and RRC. For example the NAS does not have visibility of whether the RRC has a connection or not. This potential merging of layers is assumed to be undesirable.

CN1 would like to clarify their understanding of the high level requirements for PLMN selection as follows

1. PLMN selection should not take place during ongoing NAS procedures (e.g. MM, GMM, CC, SM, SMS)
2. PLMN selection should not take place during an active CS domain call
3. PLMN selection should not take place during PS domain data transfer
4. PLMN selection should be allowed to take place during a PS domain connection where the user is not currently transferring data i.e. the user is in a low activity state
5. PLMN selection should be allowed to take place when no CS call is active and no PS data transfer is taking place

This is by no means an exhaustive list of the different scenarios, but CN1 believe it highlights the features required and that it highlights that a simple adoption of terminology from one group to the other (in either direction) is unlikely to provide the necessary clarification.

CN1 asks RAN2 to study the above list of scenarios and indicate if there are any Access Stratum activities that take place that will prevent or otherwise restrict the ability to perform PLMN selection. CN1 notes that the RRC connection status as described in the RAN2 liaison may be such an issue, but also notes that decoupling of the NAS and AS means that this is not visible to the NAS layer.

CN1 believes that Idle mode as defined in TS23.122 seems to clearly map to RRC-Idle. It also seems to be clear that 'a dedicated connection' as understood in 23.122 clearly maps to Cell_DCH state. However, it seems that Cell_FACH and Cell/URA_PCH states can be considered to be either Idle or 'connected'.

CN1 proposes that a possible interpretation is that a PLMN search is allowed provided there is no physical channel allocated to the mobile i.e. no ongoing signalling procedures or user data transfer. CN1 asks RAN2 for their opinion on such an interpretation.

CN1 will further study the issue and investigate how it may be solved, and will inform RAN2 of the progress of this work.

2. Actions:

To [RAN2] group.

ACTION: CN1 asks RAN2 group to consider the above discussion and inform CN1 whether they agree with the above stated principles.

ACTION: CN1 asks RAN2 group to consider the above discussion and inform CN1 of any further proposals they may have to solve this issue.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	China

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030896*
San Diego, California, USA, 19 – 23 May 2003

Title: LS on transport of unknown SIP signalling elements
Release: Rel-5
Work Item: IMS-CCR

Source: CN WG1
To: SA WG2, SA WG3, SA WG5
Cc:

Contact Person:
Name: Georg Mayer
Tel. Number: +358 50 48 21 43 7
E-mail Address: georg.mayer@nokia.com

Attachments:

---

1. Overall Description:

CN WG1 wants to inform, that CN WG1 has agreed to add a statement to 3GPP TS 24.229, which mandates network entities in the IM CN subsystem, which act as SIP proxies, to be transparent for the following SIP signalling elements:

- unknown SIP messages;
- unknown SIP header fields;
- unknown SIP header parameters.

The term "unknown" here makes reference to messages, header fields or parameters that are not mandatory to be supported by CSCFs in IMS Release 5.

This behaviour is a main feature of the SIP protocol as defined by RFC3261 and was implicitly mentioned in several parts of the IMS specification already, e.g. in the description of filtering in 3GPP TS 23.218. Nevertheless it was seen as necessary to put a clear statement to 3GPP TS 24.229 in order to guarantee that implementations of IMS network elements act in conformance with the SIP specification.

Transparency means here, that a network entity passes on the unknown signalling element towards the receiving user. This does not prevent the network element to perform certain actions on the unknown signalling element. For example in case of an unknown SIP request, the S-CSCF will still be able to apply filter criteria on the request.

The actions for modifications of SIP messages in 3GPP TS 24.229 have been written in a way that they apply to both, known and unknown SIP messages.

2. Actions:

To SA WG2 and SA WG3 groups.

ACTION: CN1 kindly asks SA WG2 and SA WG3 to take the transport of unknown SIP signalling elements into consideration. CN WG1 asks for a reply to this liaison statement, if any problem with this behaviour is seen from architectural or security point of view.

To SA WG5 group.

ACTION: CN1 kindly asks SA WG5 to indicate if there are any implications or possible problems regarding to IMS charging due to the transport of unknown SIP signalling elements.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030918Rev1*
San Diego, California, USA, 19 – 23 May 2003

Title: LS on Security Association Lifetimes
Response to:
Release: 5
Work Item: IMS-CCR

Source: CN1
To: SA3
Cc:

Contact Person:
Name: Kevan Hobbis
Tel. Number: +44 7782 325252
E-mail Address: kevan.hobbis@three.co.uk

Attachments: N1-030493, N1-030494, N1-030496 and N1-030646~~917~~

---

1. Overall Description:

CN1 would like to inform SA3 of agreed changes to TS 24.229 in regard to the management of security association lifetimes. These changes will appear in the next reference version of TS 24.229

CN1 have agreed changes to enhance the PCSCF behaviour regarding security association lifetimes during authentication and re-authentication. These changes allow the PCSCF to increase or decrease the security association lifetime dependent on the expiry time of still valid registrations.

The four change requests attached to this liaison show the detail of these changes.

CN1 note that this detailed operation is not aligned with 33.203 and ask SA3 to modify 33.203 to align with the agreed operation defined in the CN1 change requests.

2. Actions:

To [SA3] group.

ACTION: CN1 asks SA3 group to make the necessary changes to 33.203 to align with the operation agreed by CN1.

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	???

3GPP TSG-CN1 Meeting #29 *Tdoc N1-030~~355~~494*

Sophia-Antipolis, France, 31 March – 04 April 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **344** ⌘**rev** **1** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Setting the SA lifetime at UE upon registration
Source:	⌘	Lucent Technologies
Work item code:	⌘	**IMS-CCR**
Date:	⌘	31/03/2003
Category:	⌘	**F**
Release:	⌘	***Rel-5***

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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The SA lifetime in the UE should be set to the longest registration-expiration lifetime. Currently, the document 24.229 does not explicitly specify when the UE sets the SA lifetime and its value.
Summary of change:	⌘	Relevant text added.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	5.1.1.2 and 5.1.1.4

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

⌘

Other comments: ⌘ Revised as requested by the WG.

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.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the Authorization header, with the username field, set to the value of the private user identity;

b) the From header set to the SIP URI that contains the public user identity to be registered;

c) the To header set to the SIP URI that contains the public user identity to be registered;

d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the protected port value that is bound to the security association is known by the UE, that shall be also included in the hostport parameter;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

e) the Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network;

g) the Security-Client header field set to specify the security mechanism the UE supports, the IPSec layer algorithms the UE supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

h) the Supported header containing the option tag "path"; and

i) if a security association exists, a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity. The list contains also the identity under registration, unless this identity is barred. In order to build a proper preloaded Route header value for new dialogs, the UE shall also store the list of Service Route headers contained in the Service-Route header.

The UE shall use the registration expiration time received in the 200 (OK) response and compare it with all other locally stored registration lifetimes. The UE shall select the longest registration lifetime as the SIP level lifetime for its security association with the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

The UE shall integrity protect the REGISTER request using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration, if IK is available.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

e) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network;

g) a Security-Client header field, set to specify the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

NOTE 3: The 401 (Unauthorized) challenge sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up the security association with the UE during the same registration procedure.

h) the Supported header containing the option tag "path"; and

i) the P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity.

The UE shall use the registration expiration time received in the 200 (OK) response and compare it with all other locally stored registration lifetimes. The UE shall select the longest registration lifetime as the SIP level lifetime for its security association with the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

3GPP TSG-CN1 Meeting #29 *Tdoc N1-030~~357~~496*

Sophia-Antipolis, France, 31 March – 04 April 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **346** ⌘ **rev** **1-** ⌘ Current version: **5.4.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	SA liftime upon network initiated de-registration
Source:	⌘	Lucent Technologies
Work item code:	⌘	**IMS-CCR**
Date:	⌘	31/03/2003
Category:	⌘	**F**
Release:	⌘	***Rel-5***

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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	When the network de-registers a given public user identity, and if there are other remaining public user identities registered, the UE and P-CSCF should update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities. Currently, the document 24.229 does not explicitly specify this procedure.
Summary of change:	⌘	Relevant text added.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	5.1.1.7 and 5.2.5.2

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

Other comments:	⌘	Revised as requested by the Nokia.

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.

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) with the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated", the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the reregistration procedure as described in subclause 5.1.1.4.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF.

If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated", the UE shall remove the security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the NOTIFY request terminates.

NOTE 1: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the registration event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

NOTE 2: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.2.3, including one or more <registration> element(s) with the state attribute set to "terminated" the P-CSCF shall remove all stored information for these public user identities.

If there are no more public user identities registered, the P-CSCF shall delete the security associations and related keys it may have towards the UE.

If there are other remaining public user identities registered, the P-CSCF shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities that utilse this security association.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered), the P-CSCF shall remove the security associations towards the UE.

NOTE: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030646*
San Diego, California, USA, 19 - 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **398** ⌘**rev** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Combined CRs: N1-030495 (Lucent), N1-030558 (Nokia), and N1-030559(Nokia)
Source:	⌘	Nokia, Lucent Technologies
Work item code:	⌘	**IMS-CCR**
Date:	⌘	12/05/2003
Category:	⌘	**F**
Release:	⌘	***Rel-5***

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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The CRs N1-030495, N1-030558, and N1-030559 were addressing different issues in the subclause 5.2.5.1 of the document TS 24.229. To facilitate the inclusion of the respective CRs into the document TS 24.229, this CR combines all three CRs into a single CR.
Summary of change:	⌘	The text in the CRs N1-030495, N1-030558, and N1-030559 were combined together.
Consequences if not approved:	⌘	The editor will have to incorporate each individual CR into the 24.229 document.

Clauses affected:	⌘	5.1.1.6 and 5.2.5.1

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

Other comments:	⌘	Revised as requested by Nokia.

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.

5.1.1.6 Mobile-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

The UE shall integrity protect the REGISTER request using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration, if IK is available.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the Authorization header, with the username field, set to the value of the private user identity;

b) the From header set to the SIP URI that contains the public user identity to be deregistered;

c) the To header set to the SIP URI that contains the public user identity to be deregistered;

d) the Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected port value bound to the security association;

e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network; and

g) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

The UE shall release all dialogs prior to deregistering the last registered public user identity.

If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF. ~~If there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.~~

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) for the REGISTER request of the last registered public user identity, the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall:

1) remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information; and

2) check if the user has left any other registered public user identity. Due to that, the P-CSCF shall:

- i~~I~~f there are other remaining public user identities registered, ~~the P-CSCF shall~~ update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities; or

- i~~I~~f ~~When~~ all ~~of the~~ public user identities of a user are deregistered~~, the P-CSCF shall,~~

  ~~-~~ remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.~~; and~~

  - ~~if the subscription to the reg event package for that user is still alive, terminate the subscription to the reg event package for that user by sending a SUBSCRIBE request with an Expires header containing a value of zero. The P-CSCF shall also remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.~~

NOTE 1: Deleting a security association is an internal procedure of the P-CSCF and does not involve any SIP procedures.

NOTE 2~~1~~: There is no requirement to distinguish a REGISTER request relating to a registration from that relating to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

NOTE 3~~2~~: When the P-CSCF has sent the 200 (OK) for the REGISTER request of the last registered public user identity, the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030933***
San Diego, California, USA, 19 – 23 May 2003

Title: LS on security solutions for the Ut reference point
Response to: N1-030780 = S3-030302 LS on security solutions for the Mt reference point from SA3
Release: Rel-6
Work Item:

Source: CN1
To: SA3
Cc: SA2

Contact Person:
Name: peter.leis@siemens.com
Tel. Number: +49 89 636 75208
E-mail Address: peter.leis@siemens.com

Attachments:

.

---

1. Overall Description:

CN1 thanks SA3 for their liaison statement on security solutions for the Mt reference point (=Ut reference point). CN1 is aware that SA3 is responsible for the security architecture in 3GPP. CN1 has discussed the issue and provides the following answer:

CN1 sees that the solutions described in the liasion are feasible. However from a CN1 point of view the solutions have the following drawbacks:

- This would be the first case where a Release-6 service in an Application Server requires the S-CSCF to be updated to Release-6 which causes backward compatibility problems.
- It is anticipated that the key derivation in the S-CSCF puts additional processing load on the S-CSCF which is multiplied by the number of application servers involved.
- CN1 thinks that registration should be used exclusively for authentication of the UE to the IMS.

During the discussion it was also mentioned that the Sh interface might be used for providing the necessary keying material to an Application Server.

CN1 will closer study the item and try to provide a solution.

2. Actions:

ACTION:
NONE

3. Date of Next TSG-CN1 Meetings:

CN1_31	25th – 29th August 2003	Sophia-Antipolis, France
CN1_32	27th – 31st October 2003	China

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030944***
San Diego, California, USA, 19 – 23 May 2003

Title:	Reply LS on R99 and later emergency calls when attached to data only network
Response to:	LS S1-030539 / N1-030579
Release:	Rel-6
Work Item:	EMC1
Source:	CN1
To:	SA1, SA2
Cc:	GERAN 2, RAN 2

Contact Person:

Name: **Roland Gruber**
Tel. Number: +49 89 722 46396
E-mail Address: roland.rg.gruber@siemens.com

Name: **Atle Monrad**
Tel. Number: +47 372 93 665
E-mail Address: atle.monrad@ericsson.com

Attachments: -

---

1. Overall Description:

CN1 thanks SA1 for their LS that clarify questions on R99, R4 and R5 when attached to data only network. For R6, CN1 acknowledges the principle to allow support for emergency calls when attached to data only networks.

CN1 has reviewed the CR to 22.101 provided in S1-030538 and would like to raise the following questions and comments:

1. In the UE action required for the case described in section 10.3 ("... *attempt to find a connection that could support emergency calls. Note that this may or may not require change of serving network...*") the term "attempt to find a connection" is quite unclear. Does that mandate the UE to perform a service based cell selection before entering "any PLMN" search? (In CN1s opinion probably not, as there is no possibility for the UE to detect the support of voice service (see item 5), neither for the support of the PS nor CS domain.)
2. Is the UE as discussed in item 1, due to the lack of such an indicator, required to perform several call establishment attempts on all available PLMNs? This would cause a significant delay of the call setup time that is probably not acceptable at all. Furthermore, as stated in item 4 below, a PLMN reselection would cause a complete interruption of the PS service even for UEs that are capable to maintain a CS and PS connection in parallel. CN1 assumes that the intention is not to mandate any call re-attempts.
3. The table in section 10.1 does not distinguish whether a UE supports CS based voice services or not. In the case that the UE does not support CS based voice services, certain requirements are not applicable.
4. The fourth case in the table in section 10.1 ("*CS and PS capable only*") introduces a new requirement for non-IMS capable UEs. Up to now there was no requirement to change the serving network for a CS emergency call. CN1 would also like to highlight that such a change of the serving PLMN will cause an interruption of the PS service even for UEs which are capable to maintain a CS and PS connection in parallel (UMTS, A/Gb Mode class A, or A/Gb Mode-DTM). Such a requirement was estimated to cause a non-trivial change of CN1 specifications. CN1 would like to ask whether this was the intention. CN1 would also like to highlight that a CS emergency call may be established also if the UE is not attached to the CS domain. The same applies for the seventh case ("*CS and IMS capable*") in the table in section 10.1.
5. The new requirement given in section 10.3 is unclear. What is a PLMN that "*does not support voice services for the UE*"? Does this mean that the PLMN does not support CS domain at all (PS only) or the case when the PS + CS capable network offers only PS domain service for PS + CS capable UE (for whatever reason). There is no specific indicator available to the UE either for the "presence of a CS

domain", or for the support of "voice services" by the network. Is the term "*voice services*" covering both PS domain based IMS and CS domain based speech calls?

6. For CS emergency calls, the characteristics of TS11 are well defined. For IMS, the characteristics for “IMS speech calls” are unclear and should be clarified.

2. Actions:

To SA1 group.

ACTION: CN1 would like to ask SA1 to study the issues raised above and inform CN1 about the outcome of the discussion for each of the bulleted items.

To SA2 group.

ACTION: CN1 kindly asks SA2 to:

1 acknowledge that the scenario with ‘data only’ UE is incorporated into the TR 23.867.

2 take the comments raised in each bullet above into consideration for further work with this topic.

3. Date of Next TSG-CN1 Meetings:

CN1#31	25th – 29th of August 2003,	Sophia Antipolis, France
CN1#32	27 – 31 of October 2003,	???, ???