3GPP TSG-CN Meeting #26 **NP-040512**
8th – 10th December 2004. Athens, Greece.

Source: **TSG CN WG1**

Title: **CR to Rel-6 WI “SEC1-SC“ for TS 24.109**

Agenda item: **9.3**

Document for: **APPROVAL**

This document contains **1 CR on Rel-6 Work Item “SEC1-SC”**, that has been agreed by TSG CN WG1 CN#36 meeting and forwarded to TSG CN Plenary meeting #26 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
N1-042059	Authorization flag transfer between AP and AS	24.109	009	1	C	6.0.0	SEC1-SC	Rel-6

3GPP TSG-CN WG1 Meeting #36
Seoul, Korea, 15 - 19 November 2004

Tdoc ⌘N1-042059

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.109**	**CR**	**9**	⌘**rev**	**1**	⌘	Current version:	**6.0.0**	⌘

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

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Authorization flag transfer between AP and AS		
Source:	⌘	Nokia, Siemens		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	18/11/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	In addition of being able send list of user identities to a AS, the AP should be able to send also a list of authorization flags to the AS (if they are present in the application-specific USS of the subscriber).
Summary of change:	⌘	The AP is able send authorization flags to the AS by adding HTTP header "X-3GPP-Authorization-Flags" to each HTTP request coming from a UE to a particular AS. The list of authorization flags is comma (,) separated and each flag is surrounded by quotation marks (").
Consequences if not approved:	⌘	The AP is not able send authorization flags to AS.

Clauses affected:	⌘	2, 7.3, G (new annex added)				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 33.222 CR 010r1
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN CHANGE =====

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[2] 3GPP TR 33.919: "Generic Authentication Architecture (GAA); System description".

[3] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Protocol details".

[4] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[5] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[6] IETF RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[7] 3GPP TS 23.003: "Numbering, addressing and identification".

[8] IETF RFC 3023: "XML Media Types".

[9] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[10] IETF RFC 3548: "The Base16, Base32, and Base64 Data Encodings".

[11] IETF RFC 2246: "The TLS Protocol Version 1.0".

[12] IETF RFC 2818: "HTTP over TLS".

[13] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[14] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[15] IETF draft-ietf-tls-psk-01: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[16] PKCS#10 v1.7: "Certification Request Syntax Standard".

NOTE: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf

[17] WAP Forum: "WPKI: Wireless Application Protocol; Public Key Infrastructure Definition"

NOTE: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf.

[18] IETF RFC 3546: "Transport Layer Security (TLS) Extensions".

[19] Open Mobile Alliance: "ECMAScript Crypto Object"

NOTE: http://www.openmobilealliance.org.

[20] Open Mobile Alliance: "WPKI"

NOTE: http://member.openmobilealliance.org/ftp/public_documents/SEC/Permanent_documents/.

[21] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[22] IETF RFC 2234: "Augmented BNF for Syntax Specifications: ABNF".

===== NEXT CHANGE =====

7.3 Authorization

The AP shall be able to decide whether particular subscriber, i.e. the UE, is authorized to access a particular AS. The granularity of the authorization procedures is specified in 3GPP TS 33.222 [5].

The AP may indicate an asserted identity or a list of identities to the AS by adding a HTTP header to the HTTP requests coming from the UE and forwarded to the AS. The HTTP header name shall be "X-3GPP-Asserted-Identity" and it shall contain a list of identities separated by comma (,) and each identity is surrounded by quotation marks ("). Whether the AP adds this HTTP header to the HTTP request depends on the subscriber's GBA user security settings.

The AP may indicate an authorization flag or a list of authorization flags from the application specific user security settings (USS) to the AS by adding a HTTP header to the HTTP requests coming from the UE and forwarded to the AS. The HTTP header name shall be "X-3GPP-Authorization-Flags" and it shall contain a list of authorization flags separated by comma (,) and each authorization flag is surrounded by quotation marks ("). In case the AP supports this handling of authorization flags from USS then it shall depend on local policy in the AP.

===== NEXT CHANGE =====

Annex G (normative): 3GPP specific extension-headers for HTTP entity-header fields

G.1 General

This annex defines the syntax of 3GPP specific extension-headers introduced in this document in augmented Backus-Naur form as defined in RFC 2234 [22].

G.2 X-3GPP-Intended-Identity extension-header

The "X-3GPP-Intended-Identity" header is used optionally by the UE to indicate the user identity intended to be used with the AS. It contains the user identity surrounded by quotation marks (").

Table G.2: Syntax of X-3GPP-Intended-Identity extension-header

```
    X-3GPP-Intended-Identity = "X-3GPP-Intended-Identity" ":" DQUOTE identity DQUOTE
    identity = *(%x20-21 / %x23-7E)
```

In the syntax definition the rule 'identity' refers to the user identity and it is defined as a string of printable characters and spaces but excluding quotation marks. The exact type definition for user identity is done in TS 29.109 [3] as part of the User Security Setting definition.

G.3 X-3GPP-Asserted-Identity extension-header

Depending on the subscriber's GBA user security settings the "X-3GPP-Asserted-Identity" header is used by the AP to indicate an asserted identity or a list of identities to the AS. It contains a list of identities separated by comma (,) and each identity is surrounded by quotation marks (").

Table G.3: Syntax of X-3GPP-Asserted-Identity extension-header

```
   X-3GPP-Asserted-Identity = "X-3GPP-Asserted-Identity" ":" identity-list
   identity-list = DQUOTE identity DQUOTE *("," DQUOTE identity DQUOTE)
   identity = *(%x20-21 / %x23-7E)
```

In the syntax definition the rule 'identity' refers to the user identity and it is defined as a string of printable characters and spaces but excluding quotation marks. The exact type definition for user identity is done in TS 29.109 [3] as part of the User Security Setting definition.

G.4 X-3GPP-Authorization-Flags extension-header

The "X-3GPP-Authorization-Flags" header is used optionally by the AP to indicate an authorization flag or a list of authorization flags from the application specific user security setting (USS) to the AS. It contains a list of authorization flags separated by comma (,) and each authorization flag is surrounded by quotation marks (").

Table G.4: Syntax of X-3GPP-Authorization-Flags extension-header

```
   X-3GPP-Authorization-Flags = "X-3GPP-Authorization-Flags" ":" auth-flag-list
   auth-flag-list = DQUOTE auth-flag DQUOTE *("," DQUOTE auth-flag DQUOTE)
   auth-flag = *(%x20-21 / %x23-7E)
```

In the syntax definition the rule 'auth-flag' refers to the authorization flag and it is defined as a string of printable characters and spaces but excluding quotation marks. The exact type definition for authorization flag is done in TS 29.109 [3] as part of the User Security Setting definition.

===== NEXT CHANGE =====

Annex H~~G~~ (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
13/02/04		N1-040080			Version 0.0.1 Editor's internal draft		
13/02/04		N1-040173			TS skeleton		
13/02/04		N1-040174			Version 0.0.1 Editor's internal draft		
13/02/04		N1-040175			Version 0.0.1 Editor's internal draft		
13/02/04		N1-040176			Version 0.0.1 Editor's internal draft		
13/02/04		N1-040177			Version 0.0.1 Editor's internal draft		
19/03/04					Document updated with TS # 24.109		0.0.1
08/04/04		N1-040541			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040542			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040543			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040727			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040728			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040729			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
08/04/04		N1-040730			Version 0.1.0 incorporating results of CN1 discussions at CN1 #33bis (agreed documents N1-040541, N1-040542, N1-040543, N1-040727, N1-040728, N1-040729, N1-040730)	0.0.1	0.1.0
24/05/04		N1-040858			Version 0.2.0 incorporating the results of CN1 discussion at CN1#34 (agreed documents N1-040858, N1-041071, N1-041072)	0.1.1	0.2.0
24/05/04		N1-041071			Version 0.2.0 incorporating the results of CN1 discussion at CN1#34 (agreed documents N1-040858, N1-041071, N1-041072)	0.1.1	0.2.0
24/05/04		N1-041072			Version 0.2.0 incorporating the results of CN1 discussion at CN1#34 (agreed documents N1-040858, N1-041071, N1-041072)	0.1.1	0.2.0
21/06/04		N1-041166			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
21/06/04		N1-041236			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
21/06/04		N1-041237			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
21/06/04		N1-041239			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
21/06/04		N1-041285			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
21/06/04		N1-041286			Version 0.3.0 incorporating the results of CN1 discussion at CN1#34bis (agreed documents N1-041166, N1-041236, N1-041237, N1-041239, N1-041285, N1-041286)	0.2.0	0.3.0
26/08/04		N1-041419			Bootstrapping renegotiation indication in HTTP Digest	0.3.0	2.0.0
26/08/04		N1-041420			Key material delivery fix	0.3.0	2.0.0
26/08/04		N1-041423			Subscriber certificate enrolment to the main body	0.3.0	2.0.0

Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
26/08/04		N1-041424			HTTP Digest: B-TID, and shared secret are ASCII based	0.3.0	2.0.0
26/08/04		N1-041428			Editorial fixes	0.3.0	2.0.0
26/08/04		N1-041594			Key to interpret HTTP signalling flows	0.3.0	2.0.0
26/08/04		N1-041595			Key to interpret TLS signalling flows	0.3.0	2.0.0
26/08/04		N1-041596			Subscriber authorization at PKI portal to obtain a particular type of certificate	0.3.0	2.0.0
26/08/04		N1-041597			Subscriber certificate enrolment with WIM authentication codes	0.3.0	2.0.0
26/08/04		N1-041598			Stage 3 for authentication proxy	0.3.0	2.0.0
03/09/04					Implementation of CN1#35 CR that was incorrect in v2.0.0	2.0.0	2.1.0
03/09/04	CN-25	NP-040366			Editorial changes	2.1.0	2.1.1
08/09/04	CN-25				Editorial clean-up by ETSI/MCC (update of references and table numbers update)	2.1.1	2.1.2
2004-09	CN-25	NP-040423			The draft was approved, and 3GPP TS 24.109 was then to be issued in Rel-6 under formal change control.	2.1.2	6.0.0

===== END OF CHANGES =====