3GPP TSG SA WG3 Security#33 **S3-040319**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.9.4 (GAA/HTTPS)**

Source: **Nokia, Siemens**

Title: **Text for sub-sections 6.4 “Interfaces” and 6.5 “Management of UE Identity” within section 6 “Authentication Proxy” of TS 33.222 – Pseudo-CR**

Document for: **Discussion and decision**

Abstract

In the current version of the “Access to NAF using HTTPS” specification (TS 33.222 v100), there is no text for sections 6.4 and 6.5. During the last SA3 meeting it was decided to discuss the corresponding topics via email. This was done with a discussion paper by Siemens under the heading “[3GPP SA3 asserted ids]”. Comments and replies came from Nokia and Nortel. Based on the discussion paper and the comments the following text was generated by Nokia and Siemens.

1. Reason for proposed change to TS 33.222 v100

There has been no text up to now in the two sections. After discussions at last SA3 it was decided to start an email discussion and to clarify the topic until next SA3 meeting. This proposal is based on the outcome of the email discussion.

Section 3 contains a pseudo-CR to TS 33.222 v100, implementing the new text.

2. Comments on topics of the text

In the following some comments are given on single topics of the text. The questions and/or answers arose from the email discussion and they are given here to inform all SA3 of the background for certain decisions in the text.

2.1 Comments on section 6.4 “Reference Points”

Section 6.4.1 “Ua reference point”, second bullet in the note:
This restriction only applies if the GBA authentication itself uses Digest Authentication. For other possible authentication mechanisms, e.g. certificate based mutual authentication, use of direct authentication between UE and AS is still possible.

Section 6.4.2 “AP-AS reference point”:
Transfer of an asserted identity from AP to AS e.g. in an additional HTTP request header field is a mandatory feature. To allow interworking of APs and ASs of different suppliers the format has to be standardised in a stage 3 specification. The text explicitly states that support of this feature is mandatory for AP only. An AS may be unaware of such a transferred identity and may silently discard this information if it wants to. To support such behaviour of AS, it is suggested that stage 3 defines a format which is automatically disregarded (e.g. as invalid parameter) by any unaware AS.
NB: It is only mandatory for the AP to support this feature. It may be switched on and off in configuration per AS.

2.2 Comments on section 6.5 “Management of UE identity”

Section 6.5.1: Explanation on data sent from BSF to AP over Zn (IMPI, GAA specific user profiles):
In addition to Ks_NAF and key lifetime the BSF may send additional data to AP. This data is 1) IMPI of user, known to BSF from Ub protocol run and stored with B-TID, and 2) application specific GAA user profiles received from HSS and stored with B-TID.
Sending of the IMPI shall depend only on the configuration in BSF, while sending of user profiles depends on the applications the AP indicated in its request over Zn. Therefore all cases are possible: 1) no additional data sent, 2) only IMPI sent, 3) only requested user profiles sent, or 4) IMPI and requested user profiles sent.

Section 6.5.2.3 “Authorized user of application with transferred identity asserted to AS”:
Scenario of this sub-clause: The AP only sees the B-TID of the UE and it receives corresponding data from BSF over Zn (cf. previous paragraph). The AP does not look into the HTTP request, except for URL and/or Host request header field as any HTTP proxy does to determine which AS to proxy the request to. All data transferred from AP to AS stems only from B-TID and the corresponding data received from BSF. This in turn means that the AS cannot rely on any information contained in UE originated header fields or in the body of the message. The UE may insert here what it likes to, and the AP does no checking at all. It is solely under responsibility of the AS to correlate the asserted identity carried e.g. in the special header field inserted by AP (cf. 6.4.3) and any user identity that may be inserted by UE in other header fields or in the body of the message. But, please note, that, depending on the application, the UE may or may not insert any form of identity in the request, apart from the B-TID.

Section 6.5.2.4 “Authorized user of application with transferred identity asserted to AS and check of user inserted identity”:
Scenario of this sub-clause: This scenario extends the scenario of 6.5.3 in that the AP checks identities inserted by the UE against identities received from BSF. This means that in this scenario the AP is aware of the syntax and semantic of an application, and it knows how to interpret UE inserted identities in HTTP request header fields and/or in message bodies. Given this knowledge the AP can compare these UE inserted identities with the identities received from BSF (IMPI, perhaps IMPU from application specific user profile, or other information from application specific user profile). The AP and AS must have a policy stating which fields in the message were checked by the AP, and as a consequence, which fields the AS can rely on as authenticated.
Discussion on mandatory or optional for this case: This application specific knowledge is different for every application (e.g. Presence, Conferencing, MBMS, …). Therefore such behaviour of AP cannot be made mandatory for AP in this general specification. The best thing this specification can do is to declare such behaviour as optional.
If, for a particular application, such behaviour of AP is to be mandatory, this has to be specified in the specification corresponding to this application, not in TS 33.222. E.g., the Presence specification TS 33.141 when referencing TS 33.222 may specify an application aware proxy according to this sub-clause 6.5.2.4 as mandatory in its context.

3. Pseudo-CR

****************** 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 23.002: “Network architecture”.

[2] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”.

[3] 3GPP TS 33.220: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TR 33.919: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); System description".

[5] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence Service; Security"

[6] IETF RFC 2246 (1999): "The TLS Protocol Version 1".

[7] IETF RFC 3268 (2002): "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[8] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[9] IETF RFC 2818 (2000): “HTTP Over TLS ”.

[10] IETF RFC 2617 (1999): "HTTP Authentication: Basic and Digest Access Authentication"

[11] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)"

[12] IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1"

[13] 3GPP TS 33.210: “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security”

****************** end change ************************

****************** begin change ************************

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AP	Authentication Proxy
AS	Application Server
B-TID	Bootstrapping Transaction Identifier
BSF	Bootstrapping Server Functionality
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
NAF	Operator-controlled network application function functionality
TLS	Transport Layer Security
UE	User Equipment

****************** end change ************************

****************** begin change ************************

6.4 ~~Interfaces~~Reference points

6.4.1 Ua reference point

The Ua reference point is standardised in specification TS 33.220 [3] and in clauses 4 and 5 of this specification.

NOTE: The optional introduction of an AP has advantages which are stated elsewhere. However, the following consequences should be taken into account to decide whether an AP is to be used:

- The AP terminates TLS and HTTP digest. This relieves the AS of the burden to handle TLS and HTTP digest, but it should be noted that then the UE is not able to establish an additional end-to-end TLS tunnel to the AS , nor can the UE additionally authenticates itself to AS by use of client authentication within TLS. Furthermore, if GBA authentication uses HTTP Digest Authentication, the the UE cannot use Basic or Digest Authentication directly with AS.

6.4.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point.

NOTE: If this interface is secured or not is out of scope of this specification. IPsec over the Zb interface, as specified in TS 33.210 [13], may be applied. As AP terminates the TLS tunnel from UE, also a TLS tunnel is possible.

The AP-shall support the transfer of an identity of the UE authenticated by the AP from AP to AS in a standardised format. The format of this information element in HTTP request header is left to stage 3 specifications.

Editor’s Note: If further information elements from application specific user profile are transferred in standardised format to AS is ffs.

6.5 Management of UE identity

Different ASs need different kinds of authentication information. To support the requirements of different servers, the AP needs to perform authentication with varying granularity and with varying degree of assertion to the AS. The authentication and the corresponding assertion is therefore AS specific and has to be configured in the AP per AS.

6.5.1 Granularity of Authentication and Access Control by AP

The AP is configured per AS if the particular application or applications served by the AS is in need of an application specific user profile. This user profile may contain the public user identities.

6.5.1.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. Access is granted on success of basic GBA mechanism, i.e. the UE sends a valid B-TID and digest authentication with Ks_NAF received from BSF.

The AP is configured not to request an application specific user profile from BSF for the AS named in the request. Depending on configuration of BSF the AP may receives the private user identity (IMPI) from BSF.

This case shall be supported by AP.

NOTE: This case may apply when all subscribers of an operator, but no other users, are allowed access to operator defined services. The BSF may not send the IMPI out of privacy considerations or because the AP does not need it. If the BSF does not send the IMPI to the AP, the user remains anonymous towards the AP; or more precisely, the B-TID functions as a temporary user pseudonym.

6.5.1.2 Authorised User of Application

The AP is configured to request an application specific user profile from BSF. Depending on policy of BSF the AP receives the application specific user profile and the private user identity (IMPI) from BSF. Access is granted if allowed according to application specific user profile received from BSF.

The AP may do further checks on user inserted identities in the HTTP request if required according to subclause 6.5.2.4.

This case shall be supported by AP.

NOTE: If there is no application specific user profile configured for an application this case reduces to authentication according to subclause 6.5.1.1.

6.5.2 Transfer of Asserted Identity from AP to AS

The AP is configured per AS to perform authentication and access control according to one of the following subclauses: if required in the subclause, user identity is transferred to AS in every HTTP request proxied to AS.

Editor's Note: It is ffs if further information elements from application specific user profile may be transferred to AS.

6.5.2.1 Authorised Participant of GBA

The AP checks that the UE is an authorised participant of GBA. If the authentication of the UE by the AP fails, the AP does not forward the request of the UE to the AS.

This case shall be supported by AP.

NOTE: This case simply implies that the NAF checks that the user is known to, and has established a valid key, with the BSF, according to the GBA procedures described in TS 33.220 [3].

6.5.2.2 Authorised User of Application Anonymous to AS

The AP checks that the UE is an authorised user of the application according to application specific user profile received from BSF. No user identity shall be transferred to AS.

This case may be supported by AP.

6.5.2.3 Authorised User of Application with Transferred Identity asserted to AS

The AP checks that the UE is an authorised user of the application. The user identity (or user identities) received from the BSF shall be transferred to AS.

Depending on application specific user profile and AS-specific configuration of AP, the transferred user identity (or identities) may be the private user identity (IMPI), or taken from application specific user profile (e.g. an IMPU), or it is a pseudonym chosen by AP (e.g. Random, B-TID).

This case may be supported by AP.

NOTE: If the AP is configured to transfer a pseudonym to AS, any binding of this pseudonym to the user identity (e.g. for charging purposes by AS) is out of scope of this specification.

NOTE: If the AP is configured not to request an application specific user profile from BSF, only the private user identity (IMPI) or a pseudonym may be transferred to AS. In this case any authorised participant of GBA is supposed to be an authorised user of the application.

6.5.2.4 Authorised User of Application with Transferred Identity asserted to AS and Check of User Inserted Identity

This case resembles subclause 6.5.2.3 with the following extension:

Based on the user identity received from BSF the AP authenticates user related identity information elements as sent from UE. These "user inserted identities" may occur within header fields or body of the HTTP request.

Depending on application specific user profile and AS-specific configuration of AP, all user inserted identities (or a subset thereof) are authenticated by checking against private user identity (IMPI) or application specific user profile.

Depending on application specific user profile and AS-specific configuration of AP, the transferred user identity (or identities) may also be selected from the authenticated user inserted identities.

This case may be supported by AP.

NOTE: If AP authenticates certain or all user related identity information elements of a request, and the AS shall rely on the check of these elements, then a corresponding policy between the AP and the AS needs to be in place between AP and AS.

NOTE: Any application specific details are beyond the scope of this document and may be specified with the application, e.g. for Presence in TS 33.141 [5]. This specification does not preclude that any other application specific specification (e.g. Presence) declares this feature as mandatory in its scope.

******************end change ***************************