3GPP TSG SA WG3 Security — SA3#33 **S3-040336**
10-14 May 2004
Beijing, China

Source: **Nokia**

Title: **Pseudo-CR: Subscriber certificate based authentication in GAA**

Document for: **Discussion and decision**

Agenda Item: **GAA**

1 Introduction

This pseudo CR to TS 33.222 V1.0.0 adds a description of how to use subscriber certificates for authenticating UE towards an Application Server. This procedure is based on RFC 2246 and RFC 3268 and is part of the case in which Application Server is not using Authentication Proxy.

ANNEX: Pseudo CR to TS 33.222 V1.0.0:

===== 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)"

[Y] 3GPP TS 33.221: “Generic Authentication Architecture (GAA); Support for subscriber certificates”.

===== BEGIN NEXT CHANGE =====

5.1 Reference model:

Figure 1 shows a network model of the entities that utilize the bootstrapped secrets, and the interfaces used between them.

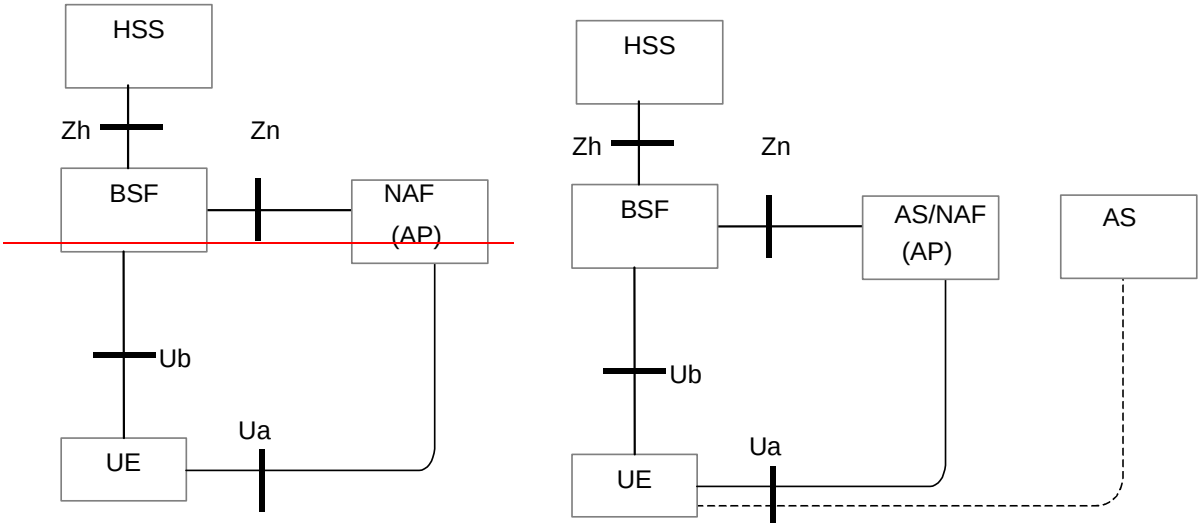

Figure 1: High level reference model for AS/NAF using a bootstrapping service (in solid line), and AS using subscriber certificates (in dash line).

NOTE: The AS may or may not support NAF functionality.

===== BEGIN NEXT CHANGE =====

5.5 Certificate based mutual authentication between UE and ~~NAF~~application server

This section explains how subscriber certificates (cf. 3GPP TS 33.221 [Y]) are used in certificate based mutual authentication between an UE and an application server. The certificate based mutual authentication between an UE and an application server shall be based TLS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

When a UE and an application server (AS) want to mutually authenticate each other based on certificates, the UE has previously enrolled a subscriber certificate as specified in 3GPP TS 33.221 [Y]. After UE is in the possession of the subscriber certificate it may establish a TLS tunnel with the AS as specified in IETF RFC 2246 [6] and IETF RFC 3546 [8].

The AS may indicate to the UE, that it supports client certificate based authentication by sending a CertificateRequest message as specificed in section 7.4.4 of IETF RFC 2246 [6] during TLS handshake. This message includes a list of certificate types and a list of acceptable certificate authorities. The AS may indicate to the UE that it supports subscriber

certificate based authentication if the list of acceptable certificate authorities includes certification authority of the subscriber certificate (i.e., operator's CA certificate).

The UE may continue with the subscriber certificate based authentication if the list of acceptable certificate authorities included the certification authority of the subscriber certificate by sending the subscriber certificate as the Certificate message as specified in section 7.4.6 and 7.4.2 of IETF RFC 2246 [6] during TLS handshake. If the list of acceptable certificate authorities does not include the certification authority of the subscriber certificate, then UE shall send a Certificate message that does not contain any certificates.

NOTE: Due to the short lifetime of the subscriber certificate, the usage of subscriber certificate does not require on-line interaction between the AS and the PKI portal that issued the certificate.

If the AS receives a Certificate message that does not contain any certificates, it can continue the TLS handshake in two ways:

- if subscriber certificate based authentication is mandatory according to AS's security policy, it shall response with a fatal handshake failure alert as specified in IETF RFC 2246 [6], or

- if subscriber certificate based authentication is optional according to AS's security policy, AS shall continue with TLS handshake as specified in IETF RFC 2246 [6].

In the latter case, if the AS has NAF functionality, the NAF may authenticate the UE as specified in subclause 5.3 of the present specification, where after establishing the server authenticated TLS tunnel, the procedure continues from step 4.

NOTE: In order to successfully establish a TLS tunnel between the UE and the AS using certificates for mutual authentication, the UE must have the root certificate of the AS's certificate in the UE's certificate store, and the AS must have the root certificate of the UE's subscriber certificate (i.e., operator's CA certificate) in the AS's certificate store. The root certificate is the root of the certification path, and should be marked trusted in the UE and the AS.

Editor's note: The support of accessing AS in the visited network is FFS in future release.

===== END CHANGE =====