3GPP TSG SA WG3 Security#32 **S3-030154**
9 – 13 February, 2004
Edinburgh, UK

Agenda Item: **6.9.2 (GBA)**

Source: **Siemens**

Title: **Deletion of parameter n – Pseudo-CR**

Document for: **Discussion and decision**

Abstract

In the current version of the Generic Bootstrapping Architecture specification (TS 33.220 v100), a parameter n is introduced to define an identity NAF_Id_n, which is input to the derivation of the key Ks_NAF. A discussion of the use of parameter n is contained in S3-040044. After further considerations, it is proposed here not to use the parameter n and always use the full DNS name of the application server as input to the derivation of Ks_NAF instead. A corresponding pseudo-CR is also included in this contribution.

1. Introduction

In the current version of the Generic Bootstrapping Architecture specification (TS 33.220 v100), a parameter n is introduced to define an identity NAF_Id_n, which is input to the derivation of the key Ks_NAF.

TS 33.220 v100, section 4.3.2, contains the following text:
"Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id_n and RAND. The NAF_Id_n consists of the n rightmost domain labels in the DNS name of the NAF, separated by dots (n= 1, ..., 7). For n = 0, NAF_Id_n equals the full DNS name of the NAF. The next bullet specifies how the UE obtains n. NOTE: This note gives an example how to obtain the NAF_Id_n: if the DNS name of the NAF is "server1.presence.bootstrap.operator.com", and n = 3, then NAF_Id_n = " bootstrap.operator.com"."

The parameter n was introduced as an option to make it possible to use only one shared key between a UE and a NAF, acting as an authentication proxy. In particular, the use of the parameter n would make it possible to use only one shared-key-TLS tunnel between a UE and a NAF, which seemed one of the main advantages of the concept of an authentication proxy.

But on the other hand, the use of this parameter n would not help to ensure the use of only one TLS tunnel in case TLS with server certificates is used between a UE and a NAF. If http digest was the Ua protocol, the advantage would then only be to have one http digest security session, instead of several. But the latter is not considered a problem in practice. Furthermore, the use of the parameter n introduces some inflexibility into the naming of application servers, and adds complexity to the system. These consequences are explained in contribution S3-040044.

It is suggested here that the disadvantages outweigh the advantages, and that the corresponding text in the specification shall be deleted. It is consequently proposed that always the full DNS name of the application server shall be used as input to the derivation of the key Ks_NAF from the key Ks. It is further proposed that a flag DER_FLAG is used to signal from the BSF to the UE whether key derivation shall be used or not.

2. Proposed Pseudo-CR

It is proposed to include the following text as a new Annex into TS 33.220:

BEGIN OF CHANGE

****

4.3.2 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure 4)

Editor's note: Zh interface related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.

Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a key update indication from the NAF (cf. subclause 4.3.3).

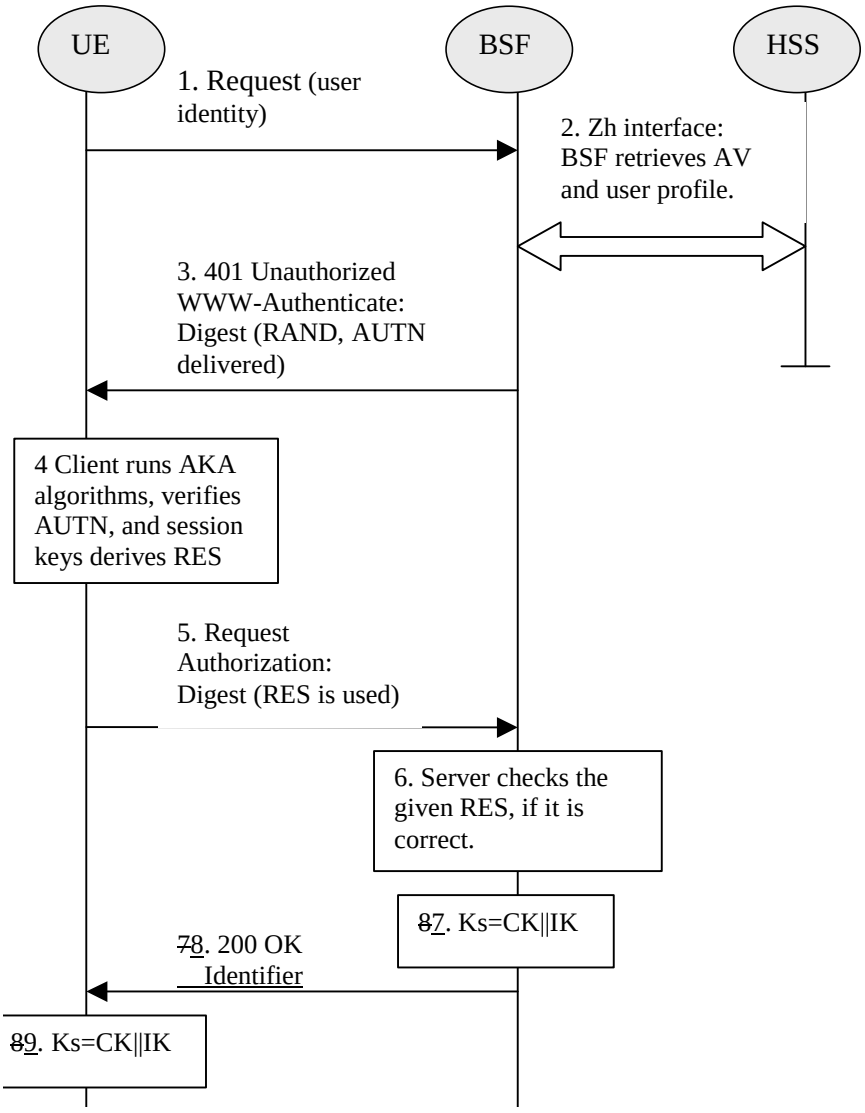

Figure 4: The bootstrapping procedure

1. The UE sends an HTTP request towards the BSF.
2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over Zh interface from the HSS.
3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.
4. The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.
5. The UE sends request again, with the Digest AKA RES as the response to the BSF.
6. If the RES equals to the XRES that is in the AV, the UE is authenticated.
7. BSF generates key material Ks by concatenating CK and IK. Ks is used to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.
8. The BSF shall send 200 OK message and shall supply a transaction identifier to the UE to indicate the success of the authentication. The BSF ~~may~~ also supplies a flag DER_FLAG to the UE, which indicates whether key derivation shall be applied to Ks or not.~~y the parameter *n* used to determine the NAF_Id_n (cf. previous bullet) to the UE over the Ub interface. If the parameter *n* is not supplied then no key derivation is performed, i.e. Ks = Ks_NAF.~~
9. The key material Ks is generated in UE by concatenating CK and IK. The Ks is used to derive the key material Ks_NAF, if applicable. Ks_NAF is used for securing the Ua interface.

Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id~~_n~~ and RAND. The NAF_Id~~_n~~ consists of the ~~n rightmost domain labels in the~~full DNS name of the NAF~~, separated by dots (n= 1, ..., 7). For n = 0, NAF_Id_n equals the full DNS name of the NAF. The next bullet specifies how the UE obtains n.~~

~~NOTE: This note gives an example how to obtain the NAF_Id_n: if the DNS name of the NAF is "server1.presence.bootstrap.operator.com", and n = 3, then NAF_Id_n = " bootstrap.operator.com".~~

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters is left to ETSI SAGE.

****

END OF CHANGE