3GPP TSG SA WG3 Security — S3#33 **S3-040317**
10 - 14 May 2004
Beijing, China

Agenda item: 6.9.2 GBA

Title: User identity transform

Source: Huawei

Document for: Discussion and Decision

1 Introduction

With the requirements and principles for bootstrapping in TS 33.220, the existing protocol and infrastructure should be reused. The Cx-interface looks like more befitting re-usage to Zh between BSF and HSS, and TS 29.109 present it more detail. The user identity in Cx-interface is IMPI, but the IMPI maybe not available in UE and the ME maybe have no ability to derive the IMPI from the IMSI. We suggest the BSF can derive the IMPI from the IMSI.

2 Discussion

The requirement to Zh interface is based on the Diameter Protocol. The diameter based implementation is based on re-usage of Cx interface Multimedia-Auth-Request/Answer messages originally between CSCF and HSS, and the TS 29.109 defines how the defined messages are used with the bootstrapping and GAA application procedures (e.g. subscriber certificates) and the application logic that is needed in GAA network elements (BSF, HSS, and NAF).

The user identity in Cx-interface is IMPI, but the GAA is generic to many services not limited to IMS, the IMPI maybe unavailable in UE.

According the TS 23.003 it shows "*If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps: ……..*" **in section 13 Numbering, addressing and identification within the IP multimedia core network subsystem.**

It's obvious If UEs want to access the IMS without ISIM, they must be able to derive the IMPI from the IMSI.

The requirements for bootstrapping "*in order to ensure wide applicability, all involved protocols are preferred to run over IP*". The services base on the IP not limit to IMS , and also include many services based on the GPRS.

Although the GAA stage 3 protocol 24.109 show: “If the UE does not have an IMS subscription, the IMPI will be constructed from IMSI”, is it reasonable?

Must those UEs they only have GPRS based services support deriving the IMPI from IMSI ?

If it is not, we suggest BSF can implement this function when UE can’t derive the IMPI from IMSI.

3 Conclusion

For the GAA can be used in generic scope and don’t preclude the limited function UE access, the BSF should have the ability to derive the IMPI from the IMSI.

4 Proposal

1 The BSF should have ability to derive the IMPI from IMSI.

2 Approve the attached CR.

5 References

[1] 3GPP TS 29.109: “Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol;
[2] 3GPP TS 23.003: “Technical Specification Group Core Network; Numbering, addressing and identification”;

[3] 3GPP TS 24.109 : “Bootstrapping interface (Ub) and Network application function interface (Ua)”

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.220 CR CRNum** ⌘ **rev -** ⌘ Current version: **V 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:	⌘	User identity transform
Source:	⌘	Huawei
Work item code:	⌘	GBA
Date:	⌘	17-04-2004
Category:	⌘	**F**
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:

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:	⌘	For the GAA can be used in generic scope and doesn't preclude the limited function UE access, the BSF should have ability to derive the IMPI from the IMSI
Summary of change:	⌘	Add "BSF shall be able to derive the IMPI from IMSI if the received user identity is IMSI" in section4.2.1 and similar description in the procedure section 4.5.2
Consequences if not approved:	⌘	The limited function UE can't access the GAA.

Clauses affected:	⌘	4.2.1 4.5.2

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

Other comments:	⌘	

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.

**********Begin of change **********

4.2 Network elements

4.2.1 Bootstrapping server function (BSF)

A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled Network Application Function (NAF). The BSF can restrict the applicability of the key material to a defined set of NAFs by using a suitable key derivation procedure. The generation of key material is specified in section 4.5.2. BSF shall be able to derive the IMPI from IMSI if the received user identity is IMSI.

Editor's note: Key generation for NAF is ffs. Potential solutions may include:
- Separate run of HTTP Digest AKA over Ub interface for each request of key material from a NAF
- Issues with key lifetime are ffs.

**********End of change **********

**********Begin of change **********

4.5.2 Bootstrapping procedures

When a UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see figure 3). 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, or when the lifetime of the key in UE has expired (cf. subclause 4.5.3).

NOTE: The main steps from the specifications of the AKA protocol in TS 33.102 [2] and the HTTP digest AKA protocol in RFC 3310 [4] are repeated in figure 3 for the convenience of the reader. In case of any potential conflict, the specifications in TS 33.102 [2] and RFC 3310 [4] take precedence.

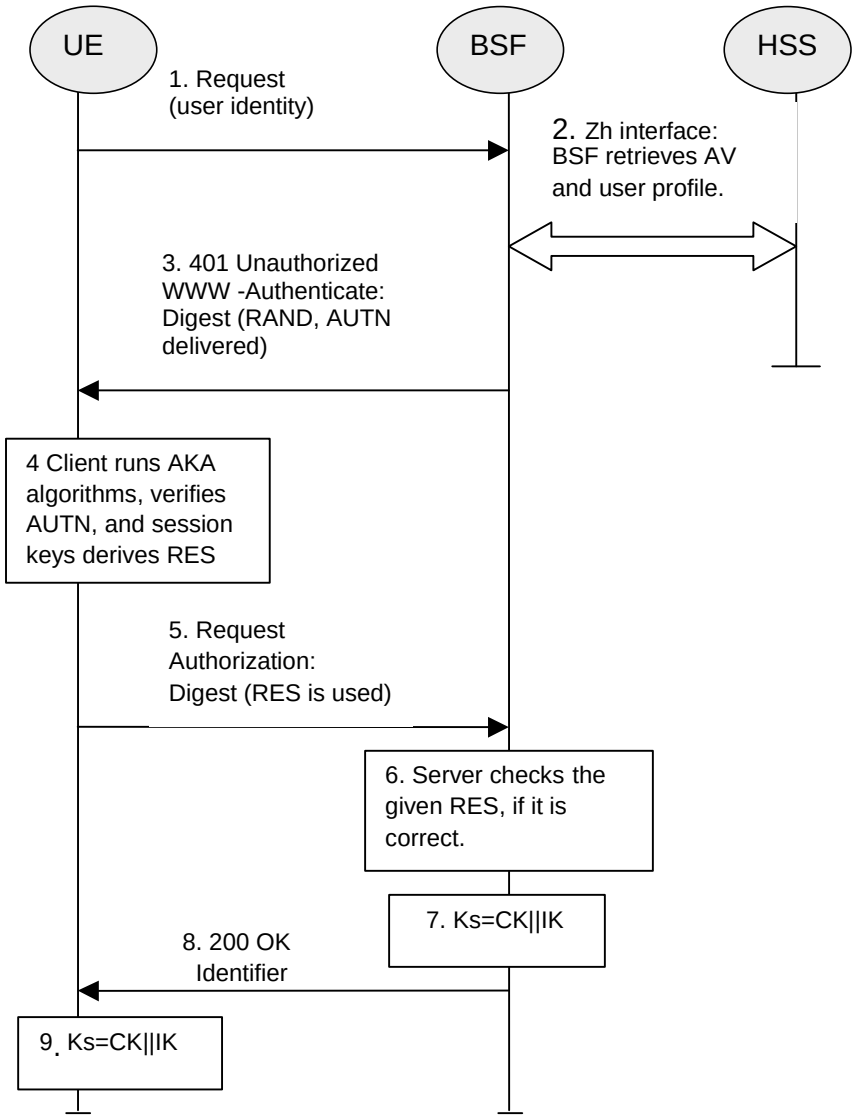

Figure 3: The bootstrapping procedure

1. The UE sends an HTTP request towards the BSF. If the received user identity is IMSI, the BSF derive the IMPI from the IMSI.

2. BSF retrieves the user profile and one or a whole batch of Authentication Vectors (AV, AV = RAND||AUTN||XRES||CK||IK) over the 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 checks AUTN to verify that the challenge is from an authorised 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 another HTTP request, containing the Digest AKA response (calculated using RES), to the BSF.

6. The BSF authenticates the UE by verifying the Digest AKA response.

7. The BSF generates key material Ks by concatenating CK and IK. The Transaction Identifier value shall be also generated in format of NAI by taking the RAND value from step 3, and the BSF server name, i.e. RAND@BSF_servers_domain_name.

8. The BSF shall send a 200 OK message, including a Transaction Identifier, to the UE to indicate the success of the authentication. The BSF also supplies a flag DER_FLAG to the UE, which indicates whether key derivation shall be applied to Ks or not. If key derivation is performed it is to be applied uniformly to all keys shared between any UE and any NAF. In addition, in the 200 OK message, the BSF shall supply the lifetime of the key Ks, and an indication whether multiple key derivation shall be used. The key material Ks is generated in UE by concatenating CK and IK.

9. Both the UE and the BSF shall use the Ks 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 and RAND. The NAF_Id consists of the full DNS name of the NAF. KDF shall be implemented in the ME.

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters are left to ETSI SAGE and to be included in the Annex B of the present specification.

If multiple key derivation is used then the UE and the BSF store the key Ks with the associated Transaction Identifier for further use, until the lifetime of Ks has expired, or until the key Ks is updated. Otherwise, the key Ks and the Transaction Identifier may be deleted in the UE and in the BSF after the key Ks_NAF has been derived.

**********End of change **********