3GPP TSG SA WG3 Security — SA3#35 **S3-040695**
October 5-8, 2004
St Paul's Bay, Malta

Source: Nokia

Title: Service discovery using default domain method

Agenda item: GBA

Document for: Discussion/Approval

1 Introduction

At SA3#34 Nokia got an action point to prepare CRs related to service discovery of BSF and PKI portal, and to use a default domain as suggested in SA2's LS S3-040373:

> "SA3 might like to consider the option of defining a default domain name for the BSF server and PKI portal of each PLMN. For example: auth.mnc123.mcc345.3gppnetwork.org and pki.mnc123.mcc345.3gppnetwork.org. These domain names can be derived by the UE from the MNC and MCC within the user's IMSI and then resolved to IP addresses using DNS."

However, SA3#35 agreed that also ISIM application may be used for bootstrapping, hence the MNC and MCC method above is not applicable is this scenario. Also, in the case where PKI portal is not in the home network is problematic as the default domain method only provides means to discover the network element in the home network. This contribution discusses how the service discovery using default domain method should be using in both for USIM and ISIM cases, and whether this method is applicable for discovering the PKI portal.

2 Discussion

2.1 Home network domain derivation

2.1.1 USIM case

In the USIM case, the FQDN for the BSF and PKI portal service discovery shall be similar to home network domain name derivation specified in 3GPP TS 23.003, subclause 13.2. The change is that in step 3, instead of adding the label "ims." to the beginning of the domain name, the label "bsf." or "pki-portal." is added. Thus the procedure would be the following:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
3. add the label "bsf." or "pki-portal." to the beginning of the domain.

An example of a home network domain name is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999,

Which gives the BSF and the PKI portal addresses:

- "bsf.mnc015.mcc234.3gppnetwork.org" for the BSF, or
- "pki-portal.mnc015.mcc234.3gppnetwork.org" for the PKI portal.

2.1.2 ISIM case

In the ISIM case, the FQDN of the BSF and the PKI portal the domain name of the IMPI is used in derivation:

1. extract the domain name from the IMPI;
2. add the label "bsf." or "pki-portal." to the beginning of the domain.

An example of a home network domain name is:

IMPI in use: user@operator.com;

Which gives the BSF and the PKI portal addresses:

- "bsf.operator.com " for the BSF, or
- "pki-portal.operator.com " for the PKI portal.

2.2 Analysis

The following assumptions must be true for the default domain method:

- the network element must always reside in the home network;
- the application in the UE deriving the address must have knowledge which application was used in bootstrapping: USIM or ISIM; and
- the application in the UE deriving the address must have access to corresponding identities: IMSI or IMPI.

Since the BSF always resides in the home network, and the application implementing the bootstrapping in the UE knows which application is being used (USIM or ISIM), this default domain method may be used for discovering the BSF.

However, it may be that the PKI portal does not reside in the home network, and the application implementing the subscriber certificate enrolment in the UE does not know which application was used during bootstrapping procedure, and it may not have access to IMSI or IMPI in question. Therefore, the default domain method should not be used for discovering the PKI portal.

3 Proposal

We propose that the default domain method described in section 2.1 is added to TS 33.220 as one of the methods for discovering the BSF. The attached CR implements the necessary changes. We also suggest that this discovery method is not used for the PKI portal.

3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040695_att1

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220** **CR** **018** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

*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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	BSF discovery using default domain method
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	06/09/2004
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:	⌘	BSF discovery using default domain method is added.
Summary of change:	⌘	The BSF address is derived from either IMSI or IMPI depending on the UICC application that was used in the bootstrapping.
Consequences if not approved:	⌘	
Clauses affected:	⌘	4.5.4

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	24.109
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘

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

4.5.4 Procedure related to service discovery

To enable the bootstrapping procedure, a procedure needs to be described on how to discover the location of BSF. It shall be possible to enable the terminal to be configured either manually or automatically via one of the following approaches:

- The address information shall be derived from the identity information related to the UICC application that was used during bootstrapping procedure, i.e., IMSI for USIM, or IMPI for ISIM;

  In the case where the USIM is used in bootstrapping, the address information shall be derived as follows:

  1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [1]) and separate them into MCC and MNC; if the MNC is 2 digits then a zero shall be added at the beginning;
  2. use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.3gppnetwork.org" domain name;
  3. add the label "bsf." to the beginning of the domain.

  Example 1: If IMSI in use is "234150999999999", where MCC=234, MNC=15, and MSIN=0999999999, the BSF address would be "bsf.mnc015.mcc234.3gppnetwork.org".

  In the case where ISIM is used in bootstrapping, the address information shall be derived as follows:

  1. extract the domain name from the IMPI;
  2. add the label "bsf." to the beginning of the domain.

  Example 2: If the IMPI in use is "user@operator.com", the BSF address would be "bsf.operator.com ".

- The address information shall be published via reliable channel. Subscribers shall store all the parameters as part of the initial establishment of IP connectivity. The addresses need to be input only once;

- The address information shall be pushed automatically to the UE over the air interface when the subscription to bootstrapping service is accepted. All the parameters shall be saved in the UE and used the same manner as above. The procedure is specified in [7];

- The location information shall be discovered automatically based on DHCP, after the IP connectivity has been established. The DHCP server shall provide the UE with the domain name of a BSF and the address of a Domain Name Server (DNS) that is capable of resolving the Fully Qualified Domain Name (FQDN) of the BSF. The procedure is specified in TS 23.228 [8].

NOTE: The location of DHCP server may be pushed to UE through the procedure specified in [7].

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