3GPP TSG-SA WG3 Meeting S3#33
Beijing, China, May 10-14, 2004

Tdoc ⌘S3-040335

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **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:	⌘	NAF's public hostname verification
Source:	⌘	Nokia
Work item code:	⌘	SSC-GBA
Date:	⌘	02/05/2004
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:

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:	⌘	NAF is able to send its public hostname (visible to UE but necessarily for BSF) to BSF so that BSF is able to derive the NAF specific key material Ks_NAF. The change in the Zn interface is NAF is able to send its public hostname to BSF. This is needed for key derivation purposes.
Summary of change:	⌘	BSF needs to have access to NAF's public hostname in order to be able to derive the NAF specific key material.
Consequences if not approved:	⌘	BSF may not able to derive the NAF specific key material, the public address of the NAF is different than the NAF internal address used between NAF and BSF.

Clauses affected:	⌘	3.2, 4.2.1, 4.3.6, 4.5.3

Other specs affected: ⌘	Y	N		⌘
	X		Other core specifications	Draft TS 29.109
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

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

3.2 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
BSF	Bootstrapping Server Function
CA	Certificate Authority
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
HSS	Home Subscriber System
IK	Integrity Key
KDF	Key Derivation Function
MNO	Mobile Network Operator
NAF	Network Application Function
PKI	Public Key Infrastructure

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

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.

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.

In addition, BSF shall be able to verify that a NAF is authorized to use a hostname, i.e., the FQDN used by UE when it contacts the NAF.

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

4.3.6 Requirements on Zn interface

The requirements for Zn interface are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BSF and NAF are located within the same operator's network.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request containing NAF's public hostname to the BSF;
- The BSF shall be able to send the requested key material to the NAF;
- The NAF shall be able to get the subscriber profile information needed for security purposes from BSF;
- The BSF shall be able to indicate to the NAF the lifetime of the key material.

Editor's note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

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

4.5.3 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in figure 5.

UE starts communication over Ua interface with the NAF:

- in general, UE and NAF will not yet share the key(s) required to protect Ua interface. If they already do (i.e. if a key Ks_NAF for the corresponding key derivation parameter NAF_Id_n is already available),, the UE and the NAF can start to securely communicate right away. If the UE and the NAF do not yet share a key, the UE proceeds as follows:
  - if a key Ks is available in the UE, the UE derives the key Ks_NAF from Ks, as specified in clause 4.5.2;
  - if no key Ks is available in the UE, the UE first agrees on a new key Ks with the BSF over the Ub interface, and then proceeds to derive Ks_NAF;
- if the NAF shares a key with the UE, but an update of that key is needed, e.g. because the key's lifetime has expired, it shall send a suitable key update request to the UE and terminates the protocol used over Ua interface. The form of this indication may depend on the particular protocol used over Ua interface (cf. 4.5.1);
- the UE supplies Transaction Identifier to the NAF, in the form of a Transaction Identifier, to allow the NAF to retrieve specific key material from BSF;
- the UE derives the keys required to protect the protocol used over Ua interface from the key material, as specified in clause 4.3.2;

NOTE: The UE shall adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any keys Ks and Ks_NAF shall be deleted from storage;
- when a new Ks is agreed over the Ub interface and a key Ks_NAF, derived from one NAF_Id, is updated, the other keys Ks_NAF, derived from different values NAF_Id, stored on the UE shall not be affected;

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to Transaction Identifier supplied by the UE to the NAF used over Ua interface;
- With the key matrial request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able verify that NAF is authorized to use that hostname;
- The BSF derives the keys required to protect the protocol used over Ua interface from the key material Ks and the key derivation parameters, as specified in clause 4.5.2, and supplies to NAF the requested key material Ks_NAF, as well as the lifetime time of that key material. If the key identified by the Transaction Identifier supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a key update request to the UE.

NOTE: The NAF shall adapt the key material Ks_NAF to the specific needs of the Ua interface in the same way as the UE did. This adaptation is outside the scope of this specification.

NAF continues with the protocol used over the Ua interface with the UE.

Once the run of the protocol used over Ua interface is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use Ua interface in a secure way.

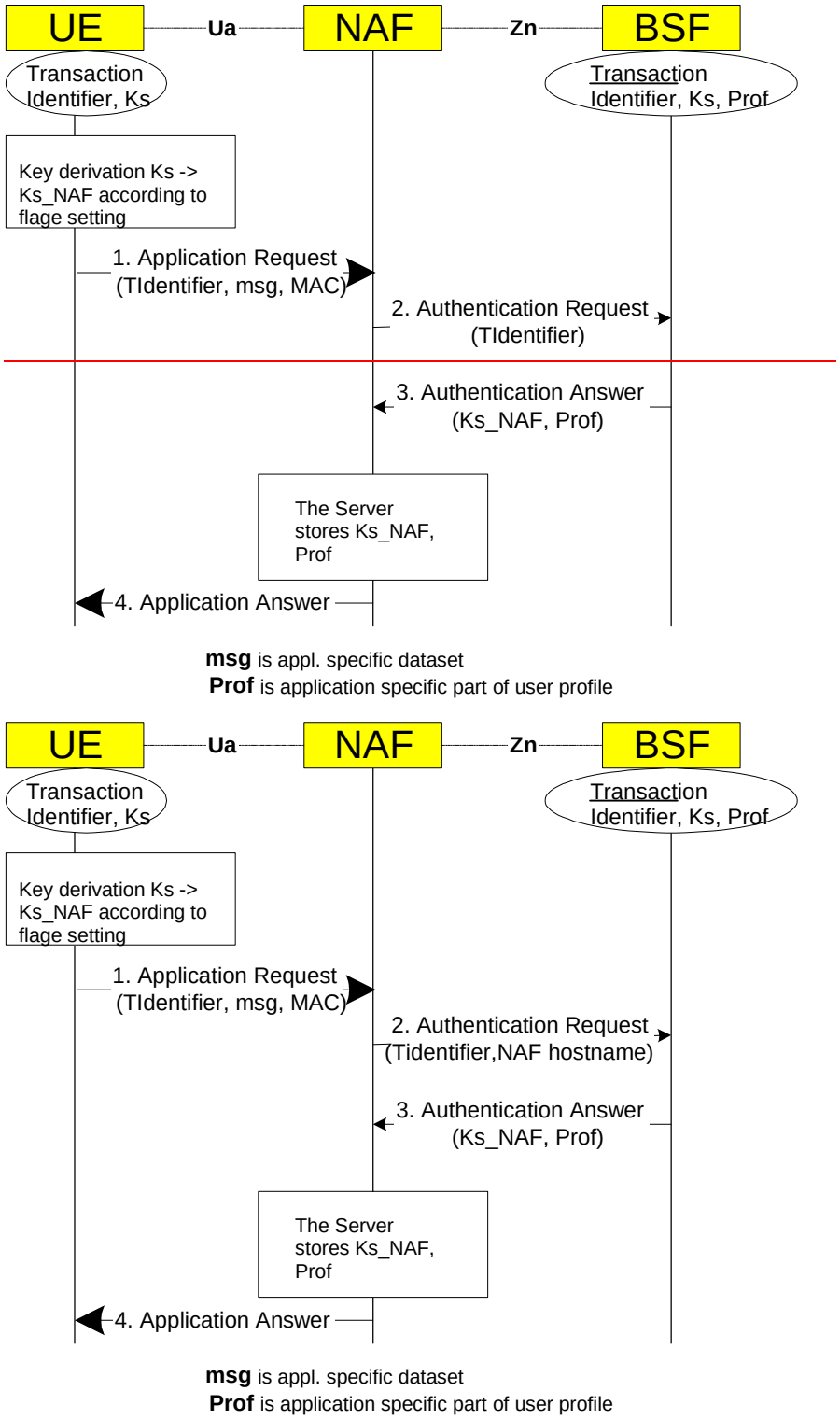

Figure 5: The bootstrapping usage procedure

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

3GPP TSG SA WG3 Security — SA3#33 **S3-040xxx**
10-14 May 2004
Beijing, China

Source: **Nokia**

Title: **NAF's public hostname**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

This contribution identifies a need where the public identity of NAF (i.e., public hostname of NAF that UE uses when contacting NAF) is explicitly sent over Zn interface to BSF in order for BSF to be able to derive the NAF specific key material Ks_NAF. This is especially necessary if NAF is doing virtual name based hosting, in which case UEs can contact one NAF by using different hostnames.

2 Discussion

It may be that the network element that is hosting a NAF has more than one network interfaces: one for serving incoming connections from UEs (i.e., "public" or "external" network interface), and one for connecting to operator services such as BSF (i.e., "internal" network interface). The address of internal network interface in Zn interface is added by the NAF to the "Origin-Host" field in Diameter message. However, the address of the external network interface of NAF (i.e., NAF's public address) is not currently conveyed to BSF from NAF. An AVP for transporting this information from NAF to BSF is needed. The external address is needed in BSF because BSF needs to be able to derive the NAF specific key material (Ks_NAF) from the fully qualified domain name (FQDN) of the NAF that UE uses (i.e., the public address of NAF). Note that BSF needs to be able to check that NAF identified by the internal address used in Zn interface (NAF_id_Zn) is authorized to use the external address using in Ua interface (NAF_id_Ua).

The need for transfer of the address of the public network interface is more evident if NAF is doing virtual named based hosting (e.g., DNS is configured so that multiple hostnames are mapped to a single IP address). Because in this case UEs can access single NAF using several hostnames, NAF needs to be able to indicate to BSF case by case what is the public NAF address that should be used in the key derivation.

SA3 is asked to endorse that the public hostname of the NAF shall be transported from NAF to BSF, and BSF shall be able to verify the mapping between the public and internal NAF identifiers.

3 Zn interface details

The messaging details between NAF and BSF over Zn interface are explained in this section.

Before Zn interface messaging takes place, UE has requested a service from NAF over Ua interface. With this request, UE has given a B-TID, and possibly a user identifier UID. Note that user identifier may also be transported from UE to NAF in later messages.

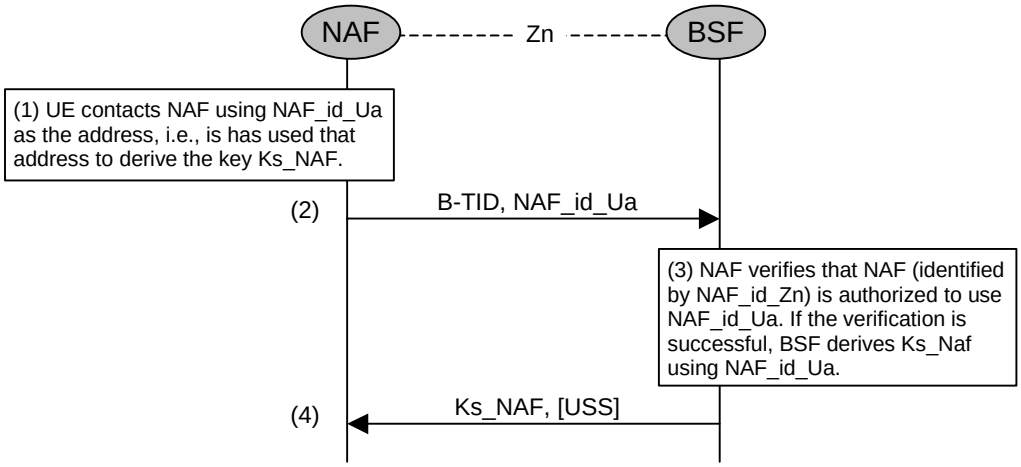

Figure 1. Zn interface diameter messages ('[ ]' indicates optionality).

Figure 1 describes the messages sent over Zn interface:

(1) UE contacted NAF using a public address of the NAF, and given the B-TID identifying the bootstrapping session.

Note: If NAF is doing virtual named based hosting; UEs can contact one NAF using several public addresses.

(2) NAF sends the B-TID and the public address of the NAF (NAF_id_Ua) to BSF.

(3) BSF verifies that the NAF is authorized to use public address.

The details of NAF_id_Zn to NAF_id_Ua mapping verification in BSF is FFS, but for example BSF may have an internal table containing the valid NAF_id_Zn to NAF_id_Ua mappings.

If the mapping verification succeeds, BSF derives the Ks_NAF using NAF_id_Ua.

(4) BSF sends the Ks_NAF and NAF specific USS to NAF. Note that NAF may not have USS, thus USS AVP is optional.

After receiving Ks_NAF, NAF can complete the authentication procedure.

If B-TID cannot be found in BSF or if the verification of the binding between NAF_id_Ua and NAF_id_Zn fails, BSF shall return an error message to NAF in step 4.

4 Conclusion

There are several reasons to transfer public hostname of NAF explicitly from NAF to BSF:

- the physical network element hosting a NAF may have more than network interface, i.e., the public hostname of the NAF may differ from the one that is used internally between NAF and BSF;
- NAF may implement virtual name based hosting, i.e., the same physical server hosting the NAF can be addressed by UEs using several hostnames.

Therefore, this contributions suggests that the following features are added to Zn interface:

- NAF is able to send the public NAF identifier used by UE over Ua interface (i.e., the public hostname of NAF that UE uses) to BSF, so that BSF is able derive the Ks_NAF.

5 Proposal

SA3 is asked to endorse that the public hostname of the NAF shall be transported from NAF to BSF, and BSF shall be able to verify the mapping between the public and internal NAF identifiers.

The attached CR implements the necessary changes in TS 33.220.