3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040647

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Securing Zn reference point
Source:	⌘	Siemens, Nokia
Work item code:	⌘	GBA and SSC
Date:	⌘	8/07/2004
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:	⌘	The Zn reference point is used between network elements that can be either in the same operator's network, or in different operators' networks. Thus, the method for securing the Zn reference point depend whether the Diameter connection is intra-operator or inter-operator. RFC 3588 recommends that IPsec should be used in intra-operator connections, and TLS should be used in inter-operator connections. This recommendation is taken into use in the TS.
Summary of change:	⌘	The inter-operator Zn reference point is newly named Zn' reference point, and the Zn reference point is intra-operator. The Zn' reference point is secured using TLS, and the Zn reference point is secured by IPsec or by using proprietary means. The TLS profile for securing the Zn' reference point is specified in the new annex D.
Consequences if not approved:	⌘	The way to secure the inter-operator Zn reference point is left open.

Clauses affected:	⌘	2, 4.1, 4.4.6

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

Other comments:	⌘	

===== 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 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[3] Franks J., et al,: "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[5] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] T. Dierks, et al,: "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[7] OMA: "Provisioning Content Version 1.1", Version 13-Aug-2003. Open Mobile Alliance.

[8] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)".

[9] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[10] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[11] IETF RFC 3588 (2003): "Diameter Base Protocol".

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

4.1 Reference model

Figure 4.1 shows a simple network model of the entities involved in the bootstrapping approach, and the reference points used between them.

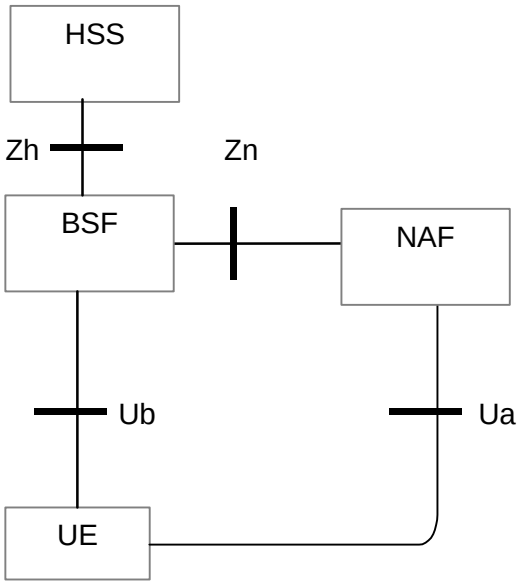

Figure 4.1: Simple network model for bootstrapping

Figure 4.1a shows a simple network model of the entities involved when the network application function is located in the visited network.

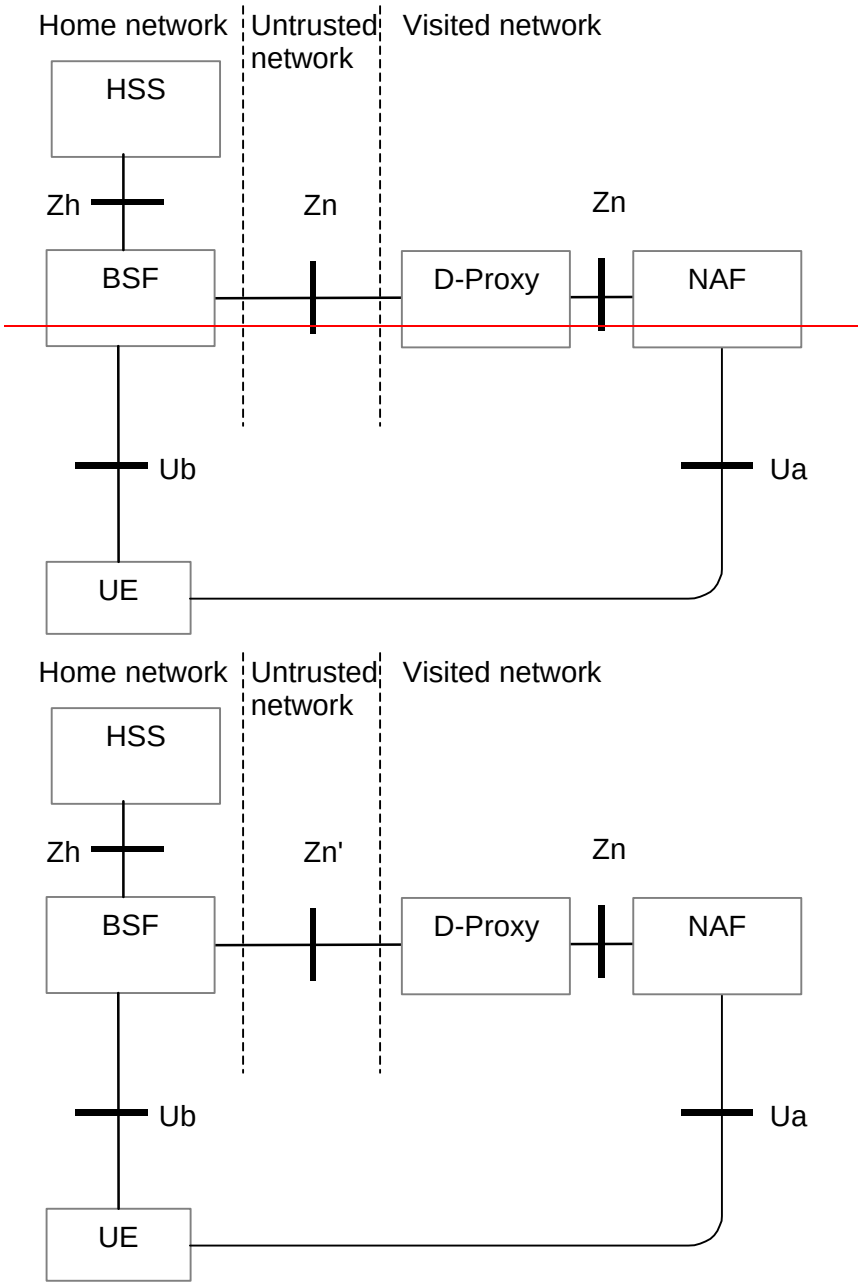

Figure 4.1a: Simple network model for bootstrapping in visited network

NOTE: The Zn' reference point is distinguished from the Zn reference point in that it is used between operators.

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

4.4.6 Requirements on reference point Zn

The requirements for reference point Zn 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.~~

~~Editors' Note: In the visited NAF scenario, it should be decided how the communication between a D-Proxy and a BSF is secured. The possible solutions for securing this link include TLS and IPsec.~~

- If the BSF and the NAF are located within the same operator's network, the Zn reference point shall be secured according to NDS/IP [10];

- If the BSF and the NAF are located in different operators' networks, the Zn' reference point between the D-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [6];

Editor's Note: The TLS Certificate profiling needs to be completed and will be added into an Annex.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request to the BSF, containing NAF's public hostname used by the UE's corresponding request. The BSF shall be able to verify that a NAF is authorized to use this hostname, i.e. the FQDN used by UE when it contacts the NAF;
- 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 reference point Ut, 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.

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