3GPP TSG-SA3 Meeting #28
Berlin, Germany, 6-9 May 2003

Tdoc ⌘S3-030231

CR-Form-v7

CHANGE REQUEST

⌘ **SpecNumber CR CRNum** ⌘**rev** **-** ⌘ Current version: **x.y.z** ⌘

*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:	⌘	Development to the draft TS contents		
Source:	⌘	Nokia		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	25/04/2003
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: ⌘ Current specification TS is just in initial form; stage 2 work should be added.

Summary of change: ⌘ This pseudo-CR develops the draft TS in the following empty sections:

- definition of certificates
- requirements on the bootstrapping function
- required functionality of the network elements
- a more descriptive figure for functionality of protocol B
- requirements on protocol D

Consequences if not approved: ⌘ Stage 2 work is missing.

Clauses affected: ⌘ 3.1, 4.1, 4.2.2, 4.3.2, 5.1.2.2

Other specs affected: ⌘

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

Other comments: ⌘

3 Definitions and abbreviations

Delete from the above heading those words which are not applicable.
Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the [following] terms and definitions [given in ... and the following] apply.

Subscriber certificate: a certificate issued to a subscriber. It contains subscriber's own public key and possibly other information such as subscriber's identity in some form.

CA certificate: A Certificate Authority signs all certificates that it issues with its private key. The corresponding Certificate Authority public key is itself contained within a certificate, called a CA Certificate.

example: text used to clarify abstract rules by applying them literally.

******NEXT CHANGE******

4 Generic AKA bootstrapping functions

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to communicate in situations where they would not be able to do so without the support of the 3GPP authentication infrastructure. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a generic bootstrapping function based on AKA protocol.

4.1 Requirements and principles for bootstrapping

Editor's note: The description of AKA bootstrapping shall be added here.

- The bootstrapping function shall not depend on the particular network application function
- The server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors.
- The server implementing the network application function needs only to be trusted by the home operator to handle derived key material.
- It shall be possible to support network application functions in the operator's home network
- The architecture shall not preclude the support of network application function in the visited network, or possibly even in a third network.
- To the extent possible, existing protocols and infrastructure should be reused.
- In order to ensure wide applicability, all involved protocols are preferred to run over IP.

4.1.1 Access Independence

Bootstrapping procedure is access independent. Bootstrapping procedure requires IP connectivity from UE.

4.1.2 Authentication methods

Authentication method that is used to authenticate the bootstrapping function must be dependent on cellular subscription. In other words, authentication to bootstrapping function shall not be possible without valid cellular subscription. Authentication shall thus be based on AKA protocol.

4.1.3 Roaming

The roaming subscriber shall be able to utilize the bootstrapping function in home network.

Editor's note: For the first phase of standardisation, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In later phases, other configurations may be considered.

4.2 Bootstrapping architecture

4.2.1 Reference model

Figure 1 shows a simple network model of the entities involved in the bootstrapping approach, and the protocols used among them.

Editor's note: The names for the reference points, A, B, C, and D need to be decided.

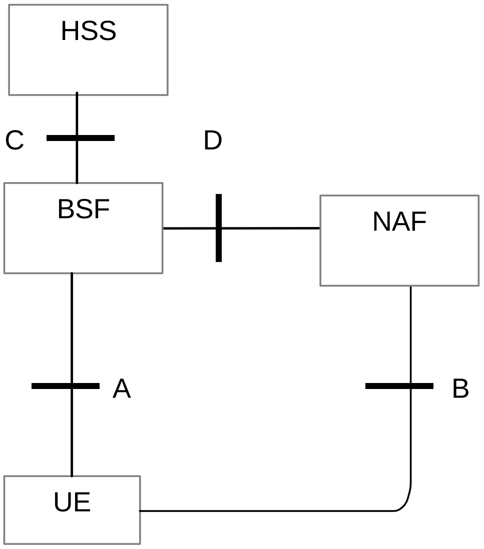


Figure 1: Simple network model for bootstrapping

Figure 2 illustrates a protocol stacks structure in network elements that are involved in bootstrapping of application security from 3G AKA and support for subscriber certificates.

Editor's note: The current protocol stack figure is placed here as a holder. The actual protocols will be defined later.

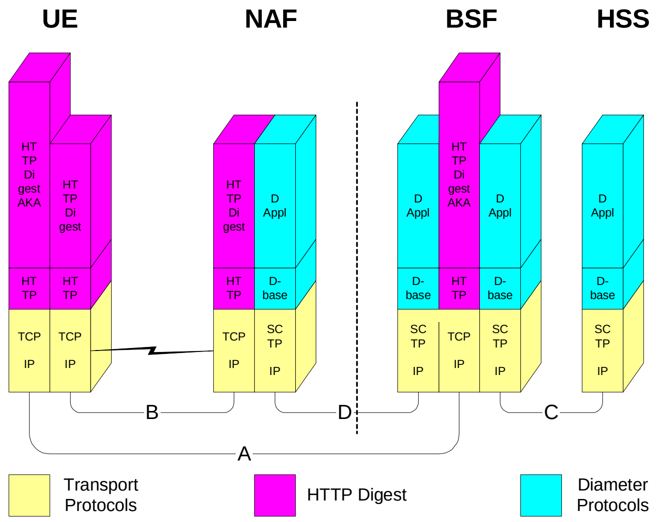


Figure 2: Protocol stack architecture

4.2.2 Network elements

4.2.2.1 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).

4.2.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled network application function (NAF) can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

General assumptions for the functionality of an operator-controlled network application function (NAF):

- There is no previous security association between the UE and the NAF.
- NAF shall able to locate and communicate securely with subscriber's BSF.
- NAF shall be able to acquire a shared key material established between UE and the bootstrapping server function (BSF) during running application-specific protocol.
- The key material must be generated specifically for each NAF independently.

4.2.2.3 HSS

HSS shall store new parameters in subscriber profile related to the usage of bootstrapping function. Possibly also parameters related to the usage of some network application function are stored in HSS.

Editor's note: Needed new parameters are FFS.

4.2.2.4 UE

The required new functionalities from UE are:

- The support of HTTP Digest AKA protocol,
- The capability to derive new key material to be used with protocol B from CK and IK, and
- Support of NAF specific application protocol (see annex A).

****** NEXT CHANGE******

4.3.2 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 ~~(see part B and D~~ in Figure4):

UE starts protocol B with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect protocol B. If they already do, there is no need for NAF to invoke protocol D.
- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.
- The UE derives the keys required to protect protocol B from the key material.

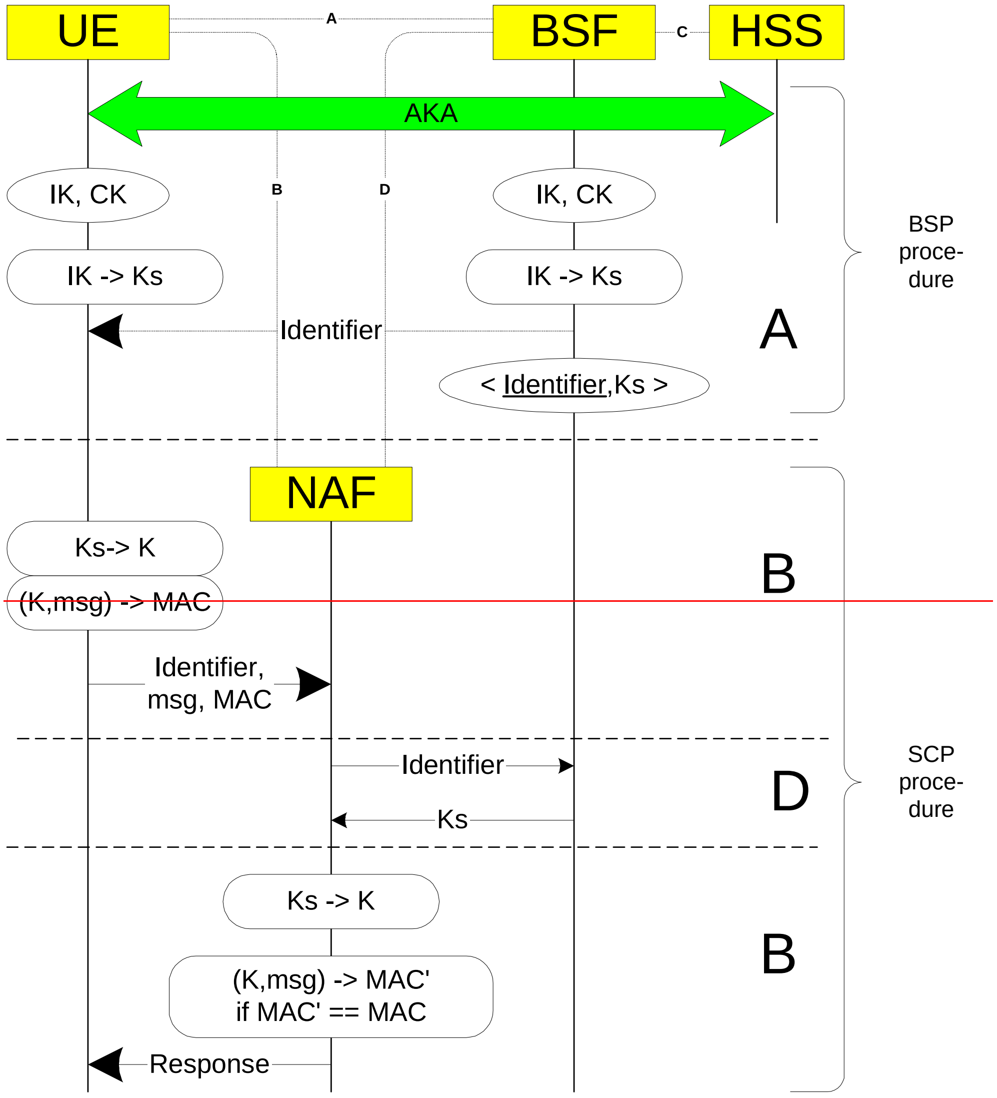
NAF starts protocol D with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of protocol B.
- The BSF supplies to NAF the requested key material.
- The NAF derives the keys required to protect protocol B from the key material in the same way as the UE did.

NAF continues protocol B with UE

Once the run of protocol B is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to run protocol B in a secure way.

Editor's note: Message sequence diagram presentation and its details will be finalized later.



MAC represents all credentials **msg** is certification appl. specific dataset

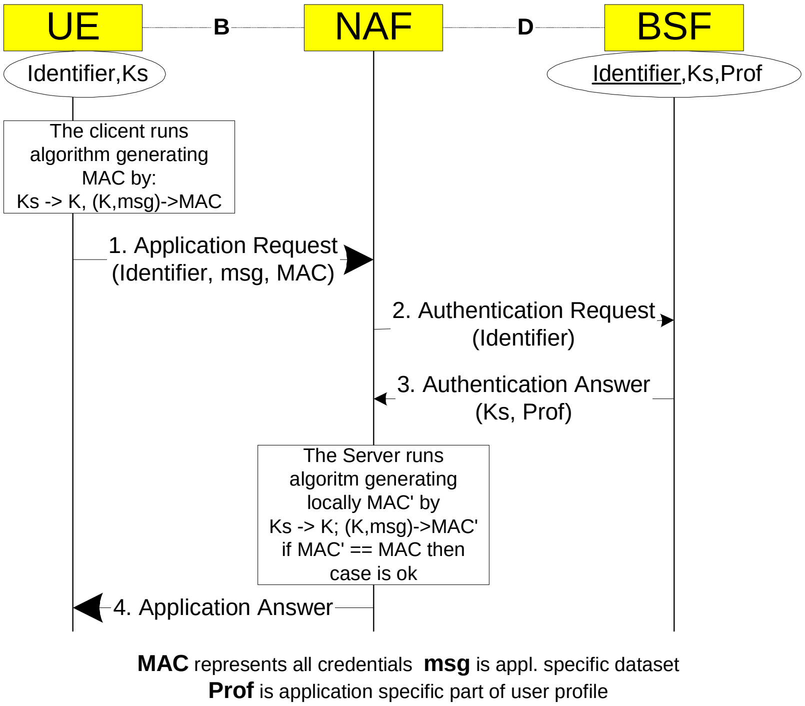

UE
B
NAF
D
BSF
Identifier,Ks
Identifier,Ks,Prof
The clicent runs algorithm generating MAC by: Ks -> K, (K,msg)->MAC
1. Application Request (Identifier, msg, MAC)
2. Authentication Request (Identifier)
3. Authentication Answer (Ks, Prof)
The Server runs algoritm generating locally MAC' by Ks -> K; (K,msg)->MAC' if MAC' == MAC then case is ok
4. Application Answer
MAC represents all credentials msg is appl. specific dataset
Prof is application specific part of user profile

Figure 4: The bootstrapping usage procedure

****** NEXT CHANGE******

5 Application specific functions using bootstrapping

5.1 Support for subscriber certificates

5.1.1 Introduction

Digital signatures can be used, for instance, to secure mobile commerce, service authorization and accounting. But digital signature by itself is not enough; there is need of a global support for authorization and charging. Thus 3GPP shall use global and secure authorization and charging infrastructure of mobile networks to support local architecture for digital signatures.

Subscriber certificates provide a migration path towards global Public Key Infrastructure (PKI). Local architecture for digital signatures can be deployed incrementally; an operator can choose to deploy independently of the others. On the other hand, the existence of subscribers and service providers that use digital signatures makes it easier to build global PKI.

3GPP systems shall issue subscriber certificates in order to authorize and account for service usage both in home and in visited network. This requires specification of:

1. Signalling procedures to issue temporary or long-term certificates to subscribers.

2. Standard format of certificates and digital signatures, e.g. re-using wireless PKI.

The mechanism shall allow a cost efficient implementation of the security support of the UE. It will also enable a user's anonymity towards the service, whilst the user who invoking the service can be identified by the network.

Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides. There is no need to standardize those services. Also, the communication between service provider and the operator (in the role of certificate issuer) need not be standardized.

5.1.2 Requirements and principles for issuing subscriber certificates

The following prerequisites for issuing of subscriber certificates exits:

- The shared key material is available for the UE application, which does the certificate request and operator CA certificate retrieval.

5.1.2.1 Requirements on protocol B

The requirements for protocol B are:

- UE is able send a certification request to NAF over a network connection.

- NAF is able to authenticate UE's certificate request.

- UE is able to request an operator CA certificate over the network connection.

- UE is able to authenticate the NAF response (i.e., operator CA certificate delivery).

- The procedure is independent of the access network used.

- The NAF should have access to the subscriber profile to check the certification policies. This means that the protocol D (cf. clause 5.1.2.2) should have support for retrieving a subset of the subscriber profile.

- The response and delivery of certificate to UE must be within a few seconds after the initial certification request.

5.1.2.2 Requirements on protocol D

The requirements for protocol D are:

- NAF is able to communicate securely with a subscriber's BSF.
- The NAF is able to send a key material request to the BSF.
- The BSF is able to send the requested key material to the NAF.
- The NAF is able to get the subscriber profile from BSF.

Editor's note: in later phases there is an additional requirement that the NAF and the BSF may be in different operators' networks