Tdoc ⌘S3-030230

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:	⌘	HTTP Digest AKA as protocol A
Source:	⌘	Nokia
Work item code:	⌘	SEC1-SC
Date:	⌘	11/04/2003
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 is to specify explicitly the HTTP Digest AKA protocol (RFC3310) as the bootstrapping protocol (protocol A).
Consequences if not approved:	⌘	Stage 2 work is missing, protocol selection is missing.

Clauses affected:	⌘	2, 4.2.3.1, 4.3			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

********* the first change**********

2 References

The following documents contain provisions that, 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*.

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TR 21.912 (V3.1.0): "Example 2, using fixed text".

[3] 3GPP TS 31.102: "Characteristics of the USIM Application".

[4] 3GPP TS 33.102: "Security Architecture".

[PKCS10] "PKCS#10 v1.7: Certification Request Syntax Standard", RSA Laboratories, May 2000.

[RFC2510] Adams C., Farrell S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[RFC2511] Myers M., et al., "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.

[RFC2617] Franks J., et al, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC 3310] A. Niemi, et al, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC3310, September 2002.

[WIM] WAP-260-WIM-20010712, 12.7.2001: http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf

[WPKI] WAP-217-WPKI, 24.4.2001: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf

********** the second change **********

4.2.3 Reference points

4.2.3.1 A

~~Protocol A is the bootstrapping authentication and key agreement protocol. It is run between the UE and the BSF and provides mutual authentication and key agreement between these entities. Protocol A is based on the 3GPP AKA [4] protocol that requires information (e.g. master key) from USIM and/or ISIM. The interface to the USIM is as specified for 3G [3].~~

The reference point A is between the UE and the BSF. The functionality is radio access independent and can be run in both CS and PS domains.

4.2.3.1.1 Functionality

Reference point A provides mutual authentication between the UE and the BSF entities. It allows the UE to bootstrap the session keys based on the 3G infrastructure. The session key as result of key agreement functionality, is used to support further applications e.g. certificate issuer.

4.2.3.1.2 Protocol

Protocol A is in format of HTTP Digest AKA, which is specified in [RFC3310]. It is based on the 3GPP AKA [4] protocol that requires information from USIM and/or ISIM. The interface to the USIM is as specified for 3G [3].

4.2.3.2 B

Protocol B is the application protocol which is secured using the session keys agreed between UE and BSF as a result of the run of protocol A. For instance, in the case of support for subscriber certificates, it is a protocol, which allows the user to request certificates from NAF.

4.2.3.3 C

Protocol C is used between the BSF and the HSS to allow the BSF to fetch the required authentication information and subscriber profile information from the HSS. The interface to the 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

4.2.3.4 D

Protocol D is used by the NAF to fetch the key material agreed in protocol A from the BSF. It may also be used to fetch subscriber profile information from BSF.

4.3 Procedures

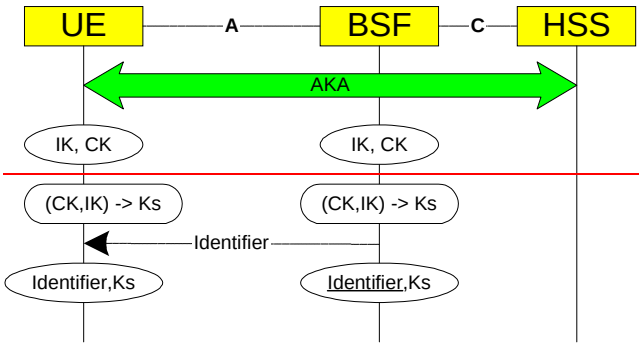
This chapter specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and latter the key agreement procedure.

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, ~~the UE~~it must ~~first run~~perform a bootstrapping authentication with the BSF ~~with the following steps~~ (see Figure 3):

~~*Editor's note: Detail message sequence diagram will be added later here to present the AKA step in concrete form.*~~

Editor's notes: Protocol C related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.



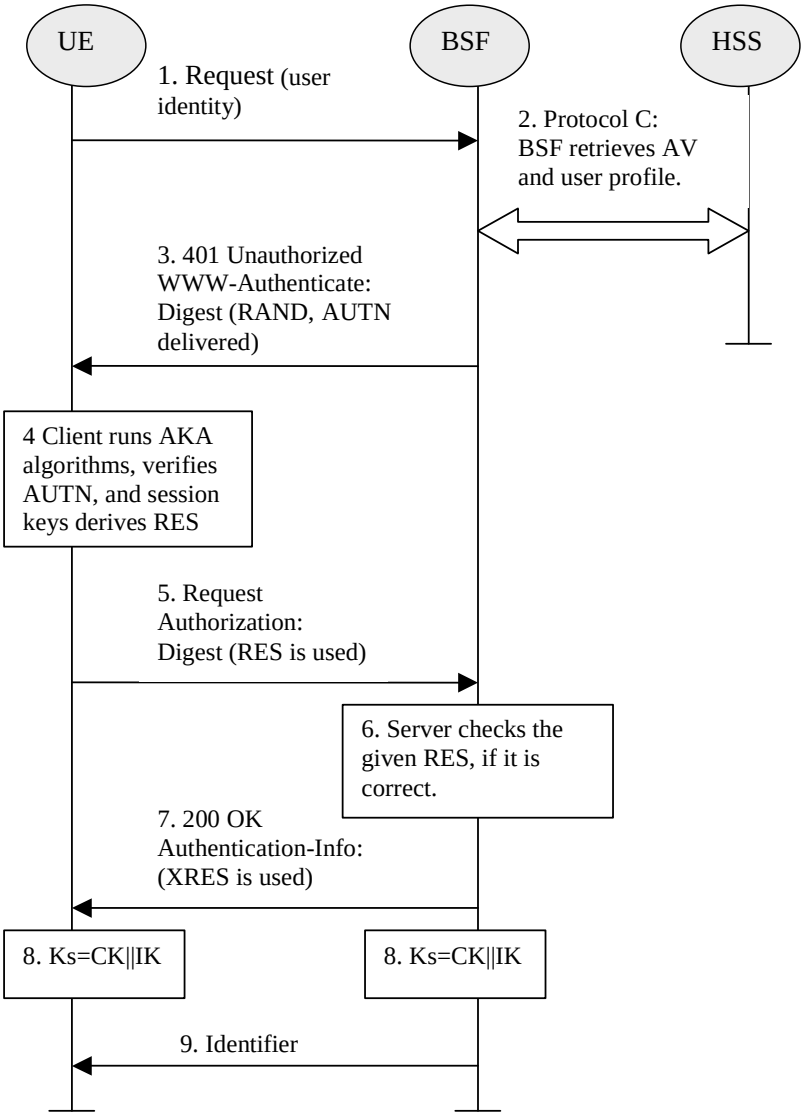


Figure 3: The bootsrapping procedure

~~UE runs protocol A with the BSF, which in turn runs protocol C with the HSS.~~

- ~~This will result in session keys IK and CK in both BSF and UE.~~
- ~~CK and IK are used in both BSF and UE to derive key material for use with protocol B. As the BSF is required to be independent of the particular application protocol B the key material is assumed to be sufficiently so that it can be used with any candidate protocol B. The key material shall not allow any NAF to infer information about CK and IK.~~
- ~~BSF may supply a transaction identifier to UE in the course of protocol A (ffs, see below).~~

1: The UE sends an HTTP request towards the BSF.

2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) by protocol C 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 calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and response RES. This will result in session keys IK and CK in both BSF and UE.

5. The UE sends request again, with the Digest AKA RES as the response to the BSF.

6: If the RES equals to the XRES that is in the AV, the UE is authenticated.

7. The BSF shall send 200 OK message to the UE to indicate the success of the authentication.

Next is the key agreement procedure:

8. The key material Ks is generated in both BSF and UE by concatenating CK and IK. The Ks is used for securing the protocol B.

9. BSF may supply a transaction identifier to UE in the cause of protocol A (ffs, see next clause).