3GPP TSG SA WG3 Security — SA3#35 **S3-040730**
October 5-8, 2004, St Paul's Bay, Malta

3GPP TR 33.cde V0.0.2 (2004-07)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects of Early IMS (Release 6)

Keywords

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal

…

Annex A:
Comparison with an alternative approach – HTTP Digest

An alternative approach is to use password-based authentication for early IMS implementations. For example, HTTP Digest (IETF RFC 2617) could be used for authenticating the IMS subscriber. This method would require a subscriber-specific password to be provisioned on the IMS terminal. Compared with the approach specified in section 7, password-based authentication has the following advantages and disadvantages:

Advantages:

- HTTP Digest is fully standardised and supported by IETF RFC 3261 (support for HTTP Digest is mandated in SIP protocol).
- HTTP Digest enables access via multiple technologies (e.g., WLAN). The solution specified in section 7 is specific to GPRS access technology.
- HTTP Digest can support partial message integrity protection for those parts of the message used in the calculation of the WWW-Authenticate and authorization header field response directive values (when qop=auth-int).
- HTTP Digest implementations can employ methods to protect against replay attacks (e.g., using server created nonce values based on user ID, time-stamp, private server key, or using one-time nonce values)

Disadvantages:

- ~~It~~ HTTP Digest may impose~~s~~ restrictions on the type of charging schemes that can be adopted by an operator. In particular, if a subscriber could find out his or her own password from an insecure implementation on the terminal, then he or she could share the IMS subscription with friends. This could impact revenue for the operator if bundled or partly subscription based tariffs are used rather than purely usage based tariffs. For example, a subscriber could take out a subscription for 100 instant messages and then share this with his or her friends. Although contractual obligations could be imposed on customers to prohibit this behaviour, in practice this would be difficult to enforce without employing special protection mechanisms, e.g., disallow multiple binding to a single IP address. If charging were purely usage based, then there would be no incentive for the subscriber to do this, therefore using HTTP Digest may ~~(and no~~not impact on operator's revenue~~)~~. The solution specified in section 7 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.
- HTTP Digest ~~It~~ provides a weaker form of subscriber authentication when compared with the levels of authentication used for other services offered over 3GPP networks, where authentication is typically based directly or indirectly on the (U)SIM. Subscription authentication depends, among other things, on the strength of the password used as well as on the password provisioning methods, such as bootstrapping passwords into the IMS capable terminal. A weak subscriber authentication, vulnerable to dictionary attacks, ~~This~~ has implications on the reliability of charging, and on the level of assurance that can be given to the customer that their communications cannot be masqueraded. In the solution specified in section 7,

authentication of the IMS subscriber is indirectly based on (U)SIM authentication at the GPRS level. The level of security is similar to that currently used for certain WAP services, where the user's MSISDN is provided by the GGSN to the WAP gateway. Security does not rely on the terminal securely storing any long-term secret information (e.g. passwords).

- HTTP Digest ~~Provisioning~~ provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed or bootstrapped into ~~in~~ each IMS terminal ~~mobile~~.

Annex B:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
29/6/04					First version based on input from S3-040264 and S3-040265.		0.0.1
8/7/04					Incorporates comments received at SA3#34.	0.0.1	0.0.2

3GPP TSG SA WG3 Security — S3#35 **Att1_S3-040730**
October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **TR 33.cde CR CRNum** ⌘ **rev -** ⌘ Current version: 6+ ⌘

*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:	⌘	Early IMS Solution – Alternative method (Annex A)
Source:	⌘	Lucent
Work item code:	⌘	Eary IMS Solution
Date:	⌘	
Category:	⌘	**D**
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 current TR does not clearly details the pros and cons of the alternative solution included in ANEX A.
Summary of change:	⌘	Adds clarifications of the advantages as well as to the disadvantages associate with using HTTP Digest as an alternative method for Early IMS implementations.
Consequences if not approved:	⌘	Operators are not presented with a complete description of an alternative method and the pros and cons associated with such a solution.

Clauses affected:	⌘	Annex A

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

Other comments: ⌘