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

Tdoc ⌘ S3-040739

CR-Form-v7.1

PSEUDO CHANGE REQUEST

⌘ **33.def** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.0.2** ⌘

*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 **X**

Title:	⌘	Adding advantages of HTTP Digest method to Annex A
Source:	⌘	Nokia
Work item code:	⌘	Security for early IMS
Date:	⌘	27/09/2004
Category:	⌘	
Release:	⌘	

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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Annex A provides a comparison with alternative approaches. A comparison should present both the advantages and disadvantages of the alternatives. Some advantages of HTTP Digest method are therefore added to Annex A.
Summary of change:	⌘	Adding some advantages of HTTP Digest approach
Consequences if not approved:	⌘	

Clauses affected:	⌘	Annex A

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

Annex A:
Comparison with alternative approaches

An alternative approach is to use password-based authentication for early IMS implementations. For example, HTTP Digest could be used for authenticating the IMS subscriber. HTTP Digest method is a widely supported authentication mechanism. It is not dependent of the GPRS network and it does not require new functional elements or interfaces in IMS network. However, t~~T~~his 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 disadvantages:

- It imposes restrictions on the type of charging schemes that can be adopted. 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. If charging were purely usage based then there would be no incentive for the subscriber to do this (and no impact on operator revenue). The solution specified in section 7 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.

- It provides a weak form of subscriber authentication 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. 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).

- Provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed in each mobile.