3GPP TSG SA WG3 Security — S3#14 **S3-000446**

2-4 August, 2000

Oslo, Norway

Source: Siemens AG

Title: Requirements on access security for IP-based services

Document for: Discussion and decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

This contribution discusses essential requirements related to the access security of the IM domain. These requirements include both security requirements and system requirements influencing the selection of security mechanism. The document also contains first considerations on the implications of these requirements which lead to working assumptions.

1. Introduction

IP-based services in UMTS Release 00 are services for which user data as well as signalling data are transmitted as IP packets in the UMTS user plane. An example for such a service is the provision of IP-based multimedia (IM) services in the IM domain of UMTS. It was decided by 3GPP to use the Session Initiation Protocol (SIP) [RFC 2543] as signalling protocol for the UMTS IM domain. The SIP messages will be carried in the user plane of the PS domain.

UMTS Release '99 security will be re-used in UMTS Release '00 to provide security at the bearer level. The confidentiality mechanism is the only mechanism which provides protection of the user plane, but its use is only optional. Only the signalling plane provides mandatory integrity. This means that the signalling for IP-based services does not enjoy the same level of protection as the signalling for other services which for carried in the signalling plane unless additional measures are specified.

The use of only bearer level security to protect the IP-based services may also prove problematic for two other reasons: one reason is that, according to the UMTS R'00 architecture principles, signalling for the IM-domain should be access network independent. Another reason is that bearer level security as specified in R'99 does not extend far enough into the core network. In R'99, only the radio access (up to the RNC) is protected. In the IM domain it may be required to extend protection of IM signalling data up to the proxy/serving CSCF (Call State Control Function) in the core network. For IM user data which is not routed via the CSCF further protection measures may be required.

2. System requirements influencing the selection of security mechanism

[TR 23.821] states certain architecture principles which imply that the UMTS R'00 architecture is to be designed to be access network independent. E.g. it is stated that “the behaviour of the multimedia call control server (CSCF) can be the same whatever the access technology (radio or wired-line) is. Multimedia call control / mobility management shall not be aware of the access technology.”

Unfortunately, [TR 23.821] is less clear regarding security. The report distinguishes between “access security functions” and simply “security functions” and states:
“Separate functions that are likely to evolve independently: The following bullets in the list are examples of major functions that may need to evolve independently. Further discussions are needed to establish an agreed list.

- . . .
- Multimedia control for multimedia sessions
- PS Mobility management, session control and access security functions
- CS Call Control, Mobility Management and access security functions
- Security functions
- . . . “

Although S3 probably has the freedom here to deviate from this independence principle for cogent reasons we believe that S3 should carefully consider such a step. This independence may prove useful when a user roams from one type of access network to a different one. It may also be useful in scenarios where the provider of the bearer service differs from that of the IM service. It is not clear at this stage, however, whether, and at what cost, this independence principle can be satisfied. It may well be, e.g., that one has to rely on bearer level security mechanisms for the confidentiality protection of IM user data when it cannot be assumed that end-to-end or end-to-gateway confidentiality protection in the IM domain is possible. Therefore we suggest the following requirement:

- **Access network independence**: Access security functions for IP-based services should be independent of the access network technology if feasible. This implies independence of the access security functions in the PS domain. If this requirement does not hold then some of the working assumptions in section 3 also have to be reconsidered.

The UMTS environment places certain restrictions on candidate security mechanisms. These include:

- **UICC aspects**

  The limits of processing power, storage capacity of a UICC and the bandwith on the UICC-UE interface have to be taken into account in the selection of mechanisms. Note that these limits are not a priori fixed, but can be extended e.g. by the use of more expensive HW (e.g. use of smart card crypto co-processors).

- **Air interface aspects**

  The air interface has limitations on the bandwidth and is error prone. This may have effects on the delay and failure rate of security procedures.

- **Network aspects**

  Any security solution must be scalable to accommodate a very large user base (up to one billion). Any security solution must support global roaming, i.e. a user must be able to get access to a serving system without previous contact between the user and the serving system.

3. Security Requirements

- **Level of protection:** For access to IP-based services at least the same level of protection shall be provided as for access to services provided in the CS- and PS-domains

This implies that the following security features shall be required for access to IP-based services:

- **Mutual authentication and key agreement** between a (roaming) user and the IM CN subsystem

  Need for three-party AKA protocol: When a (roaming) user registers in the IM domain it has to be assured that the serving IM CN subsystem corroborates the IM identity of the user, but also that the user is connected to a serving IM CN subsystem that is authorised by the user's HSS to provide IM services to him. Therefore an authentication mechanism is needed which involves three entities: UE, HSS of the user and the serving CSCF. In addition, in the course of the authentication process keys have to be agreed which can be used for the subsequent integrity and confidentiality protection of IM signalling/user data.

  There are two alternatives: rely on the UMTS AKA performed in the PS domain or perform an AKA in the IM domain. The first alternative seems not to be compatible with the requirement that the IM-domain be access network independent.

  The suggested **working assumption** therefore is the second alternative.

- **Integrity protection of IM signalling data between UE and CSCF**

  There are two alternatives to provide the required integrity

  - hop-by-hop or
  - end-to-end between the UE and the CSCF

  Hop-by-hop protection would require integrity protection of the following hops in the user plane of the PS domain.:

  - UE-RNC: This is not available in UMTS R'99, but may be available in R'00 as there is a corresponding work item. Note, however, that concerns have been raised that such protection may adversely affect Quality of Service for certain services.
  - RNC-SGSN: This is not available in UMTS R'99, but may be available in R'00 as there is a corresponding work item.
  - SGSN-GGSN: This is not available in UMTS R'99, but will may available in R'00 (GTP security).

  In addition, the hop GGSN-CSCF has to be protected which is outside the PS domain.

  Whether hop-by-hop protection is sufficient for the protection of the IM domain depends on the availability of the protection on the individual hops, the assumptions on the vulnerability of the intermediate nodes and the trust relationship between the IM domain and the PS domain. Note also that this alternative would not be compatible with the requirement that the IM-domain be access network independent.

  The suggested **working assumption** therefore is end-to-end protection between the UE and the CSCF.

- **Confidentiality of IM signalling data between UE and CSCF**

  Again, there are two alternatives to provide the required integrity

  - hop-by-hop or
  - end-to-end between the UE and the CSCF.

  Similar considerations as above apply.

  Again, the suggested **working assumption** is end-to-end protection between the UE and the CSCF.

- **Confidentiality of IM user data**

  It clearly is a requirement that user data for services in the IM domain enjoy the same degree of protection as user data for services in the PS or CS domain. The situation differs from that for signalling data in that IM user data originating from the UE do not necessarily pass through any node (such as the CSCF for IM signalling data) specific to the IM domain. E.g. in the case of a UMTS IM user communicating with a SIP user in the Internet, the IM user data will pass from the GGSN straight into the Internet. Therefore, IM domain specific protection does not seem possible in the general case. What remains is, on the one hand, end-to-end protection between users and, on the other hand, protection provided in the PS user plane. End-to-end protection between users is out of scope for the work item “access security for IP-based services”.

  The suggested **working assumption** therefore is that no additional measures need to be provided within the work item “access security for IP-based services”.

- **User identity confidentiality / user location confidentiality / user untraceability**

  A user to whom IM services are delivered needs to have a permanent identity for the IM domain. This identity or other data from which this identity may be derived or which may allow to trace the user or to derive his location (e.g. the IP address of the UE) shall not be disclosed.

  The user identity may be protected by PS domain confidentiality where it is available. Core network interfaces not contained in the PS domain need to be considered separately.

- **Secure storage of long-term keys**

  Long-term secret keying material for the protection of access to IP-based services shall be stored in only two types of security entities in the system: on the user side on a tamper-resistant HW module (the UICC) and on the network side in an Authentication Centre which is part of the HSS.

- **Secure storage and execution of cryptographic algorithms**

  All algorithms using long-term keys shall be executed on the same security entities on which the long-term keys are stored, i.e. the UICC and the Authentication Centre.

- **Transfer of session keys, storage and execution**

  The session keys for integrity and confidentiality may be transferred from the USIM to the UE where the integrity and confidentiality algorithms may be performed.

4. Reference

[TR 23.821] 3G TR 23.821: *Architecture Principles for Release 2000;* version 1.0.0, June 2000.