3GPP TSG SA WG3 Security — S3#20 **S3-010520**

16 - 19 October, 2001

Sydney, Australia

Source: **Siemens**

Title: **Requested changes to TS 33.203 v060 concerning network intitiated authenticated re-registrations**

Document for: **Discussion and Decision**

Agenda Item: **7.3**

Abstract

This contribution proposes to replace one sentence in section 5.1.1 of TS 33.203 v060 to state the requirement that a network operator shall be able to initiate an authenticated registration at any time, independent of previous registrations.The revision marks below indicate the proposed changes against TS 33.203 v060. TS 33.203 is not yet under change control, so the cover sheet for a CR is not used.

5.1.1 Authentication of the subscriber and the network

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network]

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The exact details of the subscriber profile are FFS but it will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests an IM-service the S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorization of IM-services).

All SIP-signaling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides with a transport service and QoS.

For IM-services a new security association is required between the mobile and the IM CN SS before access is granted to IM-services. The Home Network or a 3rd party even (which does not have to be an UMTS operator) provides the user with the IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAC, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and it will be reused for IM-services and then called IMS AKA.

The Home Network authenticates the subscriber at registrations or re-registrations only. ~~*In order to re-authenticate a subscriber the Home Network can force a re-registration by using e.g. a re-registration timer.*~~ Both a P-CSCF and a S-CSCF shall be able to initiate an authenticated re-registration of a user at any time, independent of previous registrations.

[Editors Note: Authentication shall according to the current requirements only take place at (Re-)Registrations.]

[Editors Note: solutions for the initiation of network initiated authenticated re-registration shall be elaborated by CN1. The stage 2 information flows shall be included in this TS 33.203.]