3GPP TSG SA WG3 Security — S3#23 **S3-020242**

14 - 17 May 2002

Victoria, Canada

Source: **Nokia**

Title: **MAC verification service for cellular subscribers**

Document for: **Discussion**

Agenda Item: **6.7**

1. Overview

In S3-020105, Nokia proposed changes to support the registration of subscriber public keys with a certification authority in the CN by sending a subscriber certificate request via the integrity-protected communication channel between UE and CN. The UE can later send credentials in the form of digital signatures to a third party service provider. The service provider will be able to verify the digital signature using subscriber certificates issued by the CN.

An alternative form of credential is a message authentication code (MAC). MACs are based on symmetric key cryptography. The protocol described in S3-020105 can be easily extended to support MAC-based credentials.

2. Changes needed to support MAC-based credentials

The first parameter in SUBSCRIBER-CERTIFICATE REQUEST message is ***key-info*** is modified as follows:

- ***key-info****: choice* of
  - ***public key***: *SubjectPublicKeyInfo* (algorithm identifier, and bitstring)
  - ***pk_hash***: *KeyIdentifier* (octet string; algorithm is SHA-1*)*
  - ***mac_key***: *MACKey* (algorithm identifier, and bit string).

When the UE wants to register a MAC key instead of a public key, it generates or chooses a MAC key, and sends a SUBSCRIBER-CERTIFICATE REQUEST with the ***key-info*** containing this key (as a ***mac_key***). The ***key-origin*** parameter in the SUBSCRIBER-CERTIFICATE REQUEST shall be 3 (to indicate that the key is from UE own memory).

When the CA in the core network receives a SUBSCRIBER-CERTIFICATE REQUEST with ***mac-key***, it shall create an entry binding the MAC key to the subscriber, and send back a it SUBSCRIBER-CERTIFICATE REPLY where the ***cert-info*** parameter is a ***subscriber certificate URL***. The URL must contain sufficient information for the core network to relate the URL to the MAC key.

The UE may use MAC-based credentials in the same way as digital signature-based credentials except that a MAC is used in place of the digital signature, and the URL received in ***cert-info*** is used in place of a certificate.

To verify a MAC-based credential, the receiver of the credential will contact the server at the specified URL and submit a message and an alleged MAC. If the alleged MAC is a valid MAC for the message under the MAC key specified by the URL, the server will send back a positive answer. For this to be useful, the receiver shall trust the server and have an appropriate security association with it.