3GPP TSG SA WG3 Security — S3#24 **S3-020365**

9 - 12 July 2002

Helsinki, Finland

Source: **Siemens**

Title: **Analysis of Subscriber Certificates Concept**

Document for: **Discussion**

Agenda Item: **7.7**

Abstract

This contribution analyses the subscriber certificates concept as was provided by Nokia in SA3#23 in Victoria [S3-020300]. First, the registration process requirements are analysed and a comparison with the WAP2 model is made. Secondly, the analysis focuses on more general aspects related to the LS from SA2 [S3-020356] to this meeting and concludes that general requirements have to be clarified first before selecting and enhancing a proposed solution.

1) Introduction on the registration process

Registration is a crucial point in the certification process. As an identity certificate binds identity-related information to a cryptographic public key, a certificate is only as good as the identification of the owner is done.

The home network provider who has already a contract with the customer can provide certificates with a relatively high trust-level without complex request- and identification-mechanisms as an identification has already be performed by the initial subscription. After this initial subscription the user can be related for instance to a mobile phone number so that the network provider has a secondary means of identification.

Service-providers not owning a customer-database are in a more unfavourable position, as they cannot rely on an already available customer-database. Depending on intended usage of the certificate, a more or less complex and trustworthy registration process is needed. Service Provider could cooperate with the home network provider to enhance the trustworthiness of the certificate if needed, but this enhances the registration procedure complexity.

Possible mechanisms for registration:

- The user has already subscribed for a mobile service. Therefore the home network provider has already done an initial identification. In the case, that a home network provider is the PKI-provider at the same time or that the PKI is hosted for the network-provider, the identification already performed can be the basis for a certification-request.
- If no former relationship existed between the PKI-provider and the user, the identification is more difficult to perform in a trustworthy way. Therefore the situation is equivalent to today's use of the Internet in an anonymous way. If the requester is not already known to the issuer the following request-processes may be considered:
  - It is only checked, whether the reply-address in the request can be reached and therefore exists.
  - An out of band mechanism is used for the registration process (phone call, mail, etc.).
  - The requester has to register in person at a local RA.

2) Registration Protocol Requirements

Protocols have been developed to automate the registration process. Examples are SCEP (Cisco Simple Certificate Enrolment Protocol), and CMP (Certificate Management Protocol- RFC 2510/11). These protocols try to minimize the needed manual interaction for certificate registration. Assuming that there is no former relationship (the internet like trust model), for initial registration, manual intervention cannot be omitted for reasons of providing an initial authentication key (by an out of band method) to bootstrap and secure the enrolment or to provide a key to be able to initiate revocation if needed later on.

The above-mentioned protocols realise the following requirements:

A) Message origin authentication (Integrity Protection) between the End Entity and the RA/CA.

The end entity is provided with a secret value (initial authentication key) and reference value (used to identify the transaction) via some out-of-band means. The initial authentication key can then be used to protect relevant PKI messages.

B) Proof of possession of key pair.

Where an end entity requests a certificate containing a given public key value, the end entity must be ready to demonstrate possession of the corresponding private key value. This is especially important for a signing key to guarantee non-repudiation of signed transactions. Proof of possession of the private signing key by the end-entity may be done by signing a challenge provided by the CA/RA. Proof of possession of keys used for encryption is performed by giving the End-entity a value to decrypt.

C) Protection against replay attacks.

Nonces within the protocol protect the recipient and sender from replay attacks.

3) Analysis of [S3-020300] and comparison to WAP-model

This clause checks the above requirement in [S3-020300] and for the concept provided by WAP2.0.

A) Message origin authentication (Integrity Protection) between the End Entity and the RA/CA.

[S3-020300]:
The integrity protection of the critical certificate data is provided only between the RNC and MT. The protection of the path between the RNC and the CA is currently unspecified but required.

[WAP20]:

In WAP20 [WAP-217_100-WPKI-20010424-a.pdf, Clause 7.3] for Over The Air Client provisioning, CMC, CMP formatting may be used and passwords to bootstrap the certification. Provided that the passwords are strong enough the WAP-model seems to be more secure, but requires user interaction which could be avoided in [S3-020300]. The password-transfer is protected via WTLS encryption. The WAP model runs completely in the user plane whereas the Nokia-model mixes user and signaling plane usage.

B) Proof of possession of key pair

According to [S3-020105], POP has to be included, but the derived Change Request [S3-020300] does not include POP provisions.

C) Protection against replay attacks.

Replay protection is realized at the RNC-MT interface by means of the Integrity protection mechanism specified in UMTS (COUNT-I) for the proposed solution [S3-020300]. For the RNC-CA interface this is currently unspecified (See A).

4) General aspects

A) Home or Visited network issuing the certificates ?

Currently [S3-020300] specifies that the operator CA is part of the Visited Network.

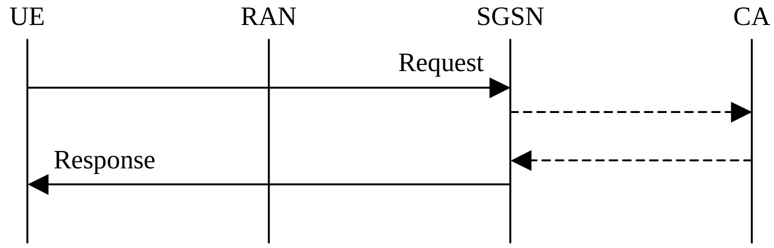

Figure 1. Certificate retrieval restricted to VN.

The user has a contractual relationship only with the home operator who bills the user and should be the only point of contact for the user in case of disputes. On the other hand, the service provider may only have a contractual relationship with the visited operator, so the latter may be in a better position to provide certificates for the service provider. The implications have to be studied further, in particular, it has to be studied whether there is an increased potential of fraud.

B) Making the Subscriber Certificate concept independent of the RAN ?

[S3-020356] (LS from SA2) asks SA3 for a justification of using a link specific access method. This contribution already tried to bring forward certain disadvantages of [S3-020300] with respect of protecting the integrity of the certification request. By definition, the certificates are to be used towards applications, so therefore is more natural to develop a concept that is link layer independent. WAP2 provides such a model and could be used as a basis for investigation.

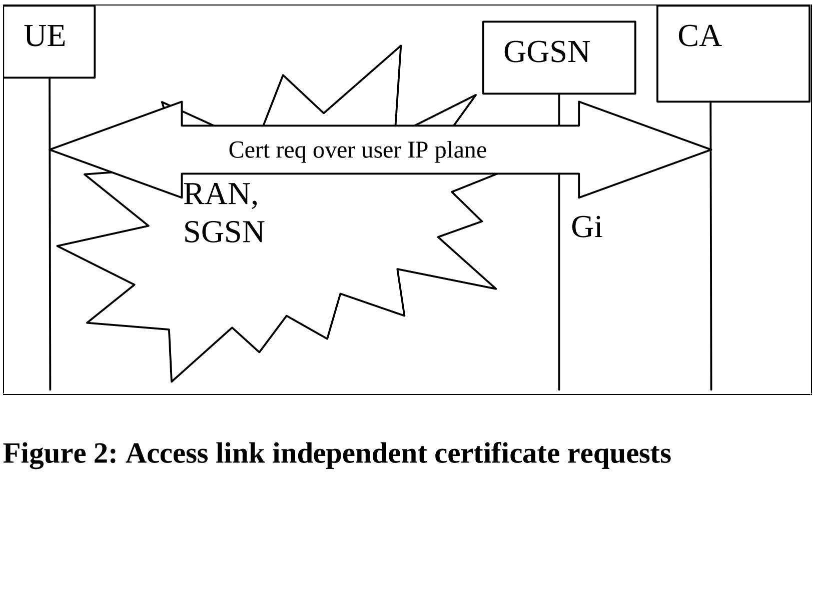

Figure 2: Access link independent certificate requests

Beside that, making use of an access link specific method (and relying on the integrity protection of it) also introduces some access link specific restrictions. As the A/Gb-mode does not have integrity protection, the concept developed in [S3-020300] cannot be used there, where using a user plane concept could do.

5) Conclusion

Siemens requests SA3 to decide on the general aspects first before going into the details of current proposals [S3-020300]. Based on the analysis of the previous chapters, it seems to be more appropriate to go for a WAP2-like model: i.e. Subscriber Certificate Request running completely in the user plane (based on IP, and using the protocols specially developed for certificate requesting) and that the Home Network shall be the responsible for issuing the Subscriber Certificates. However, in this case it has to be clarified further in how far a subscriber certificate issued by the home operator can provide sufficient assurance to a service provider in the visited domain. The technical decisions in SA3 have to be guided by requirements of SA1, which may have to be based on business scenarios. Within [S3-020356] this is also mentioned as ‘to clarify the requirement with respect to what kind of controls are required when issuing and using certificates for roaming subscribes’. Therefore SA3 needs to wait for the Response of SA1.

6) References

[S3-010353]: Support of certificates in 3GPP security architecture (first ideas of Nokia commented by Orange – SA3#19 Newbury, UK, July 2001

[S3-020077]: Usage scenarios for subscriber certificates (Nokia) – SA3#22 Bristol, UK, Feb 2002

[S3-020105]: Public key certificates for cellular subscribers (Nokia) (base doc for CR), SA3#22 Bristol, UK, Feb 2002

[SP-020119]: Revised WI on support of subscriber certificates (Rel-6) – SA#15, March 2002

[S3-020300]: CR to TS 33.102 Rel-6 Support for certificates (Nokia) – SA3#23 Victoria, Canada, May 2002

[S3-020322]: LS to SA2,CN1 on Subscriber certificates - SA3#23 Victoria, Canada, May 2002

[WAP-217_100-WPKI-20010424-a.pdf]: Wireless Application Protocol Public Key Infrastructure Definition (WAP20) http://www.wapforum.org

[S3-020356]: (S2-022047): LS (S2-021623/S3-020322) on “LS on subscriber certificates” from SA2,- SA3#24 Helsinki, Finland, July 2002