3GPP TSG SA WG3 Security **S3-020509**

8th – 11th October, 2002

Munich, Germany

Agenda Item: 7.7 Support for subscriber certificates

Source: Ericsson

Title: Issuing Subscriber Certificates at Application Layer

Document for: Discussion/Decision

1. Introduction

SA3 is currently discussing alternatives on how certificates could be issued to mobile subscribers [see e.g. S3-020300]. The main idea is to re-use the existing security association between the home network and the subscriber to protect the certificate requests. Alternative in which the visited network is issuing certificates at network layer has been most visible in SA3.

This paper discusses an alternative approach for issuing subscriber certificates at application layer. Application layer (instead of some lower layer) is preferred in order to promote access independency. For example, operators should be able to issue certificates for UMTS and WLAN users who have an AKA based trust relationship with the home network. One alternative solution is demonstrated, however, the question of a 'correct' transport protocol for certificate management messages is left open on purpose. More important is that certificate management protocols are applied in similar way over various transport protocols and accesses.

2. Trust model assumptions

SA1 has defined general requirements for subscriber certificates in their Liaison Statement [S1-021685]. The requirements include:

- The certificates shall be issued over authenticated network connection.
- The feature shall be based on existing 3GPP system security principles and mechanisms as far as possible.
- Certificate management procedures must be authenticated and integrity protected.
- It shall be possible to issue certificates for service usage both in the home and visited networks.
- It should be possible for the home operator to exercise control over service usage in the visited network.

Based on these general requirements, we assume the following kind of trust model for issuing subscriber certificates:

1) The Home Network (HN) has a first-hand trust relationship with the subscriber, and consequently only the HN should issue identity certificates to UE's public key. Authentication may be based on USIM authentication.
2) The HN has trust relationships with external Service Providers (SPs), and consequently it may issue attribute certificates to be used with these SPs.
3) The Visited Network (VN) has also trust relationships with external SPs, and consequently VN may issue attribute certificates to be used with these SPs. In this case, SPs need to use both the identity and attribute certificates to identify and authorize the subscriber.
4) If a SP has a trust relationship only with the VN and it cannot directly trust on the subscriber identities, the VN may create the trust by cross-certifying the HN to the SP. In this case, the certificate chain includes two levels: the HN has signed the subscriber certificate, and the VN has signed the HN certificate. Because SP trusts the VN, it can also trust those entities that are certified by the VN.

Full certificate management includes a wide set of functionality. One part includes issuing new certificates. There are, however, a lot of other functions, for example revocation and certificate status queries. In this paper, we focus on subscriber certificates. We assume the following requirements for subscriber certificates in 3GPP context:

- E2e protection between UE and Home Network is required.
- Application layer does not set such bandwidth limitations that Proof-of-Possession (PoP) should be ignored. We think that PoP must not be ruled out by the technical solution, and that it should be included if the certificates are needed for applications such as mobile e-commerce. Furthermore, certificates without PoP may not be trusted by some VNs or some external SPs.

3. Application layer approach

RFC 2510 describes the Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocols [RFC 2510]. Certificate management protocol messages such as certification requests, certificate status queries and revocation information, can be carried in FTP, TCP/IP, HTTP or e-mail. The basic requirement has been that the PKI management protocols must be usable over a variety of "transport" mechanisms.

The protocol messages can be protected independently from the "transport" mechanism. The use of pre-shared secrets, such as AKA generated session keys, is possible already with the existing IETF standards.

There are also other transport protocols that are able to carry MIME bodies. For example, WAP could also provide means to carry certificate management protocol messages. On the other hand, SIP is able to carry MIME bodies and consequently IMS could be re-used to carry X.509 PKI Certificate Management entities. However, the use of SIP for certificate management is probably not what IETF has had in their mind when specifying the protocols. Furthermore, re-using IMS security architecture for certificate management functionality does not add that much value because the certificate management messages can be secured independently from the transport mechanism.

We think that the transport protocol to be used for carrying certificate management messages is not the critical question. More important is to define a standard way to apply AKA generated session keys to protect the ‘transport-independent’ certificate management messages.

3.1 IMS based transport

In this chapter, we demonstrate how IMS could be re-used for issuing subscriber certificates. However, this does not conclude that we would suggest IMS as the one and only solution for the problem. Instead, we promote liberal use of different transport protocols to carry AKA protected certificate management messages.

In theory, subscriber certificates could be fetched from the home network during the IMS registration procedure. AKA RES could be used to protect the integrity of the certificate management messages in which the certificate request and the root CA certificate are carried. However, the length of AKA RES sets limitations to the trustworthiness of the end-to-end integrity protection. If a short RES is used, the integrity protection cannot be trusted. Furthermore, time required for certificate creation is most probably too long for UE to wait without re-transmissions.

SIP –specific event notifications could also provide an alternative approach to request and even maintain subscriber certificates. However, full utilization of certificate management protocols would require new SIP event types to be standardized in IETF. SIP standardization rules are very explicit that extensions for event notifications should only be done for applications that clearly need SIP. Our current understanding is that IETF does not recognize SIP event notifications as a potential protocol for certification management.

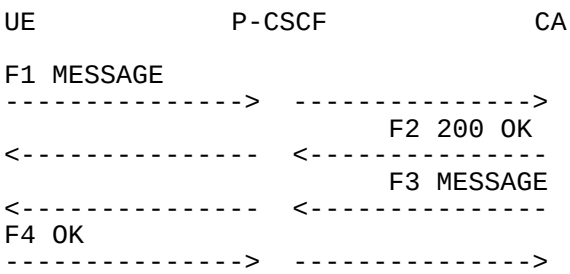
The last SIP alternative is SIP messaging. SIP messaging is able to carry short instant messages between communicating peers. It is probably the best alternative among SIP to be applied for certificate management.

The following process diagram demonstrates how SIP messaging and IMS could be re-used for certificate management:

The content of these messages are as follows:

- F1: SIP MESSAGE including HTTP Digest AKA header, and the AKA identity of the UE.
- F2: The CA challenges the UE with AKA authentication challenge.
- F3: Second MESSAGE including the HTTP Digest AKA response. The certification management body is protected using AKA session key. The body includes signed certification request from the UE.
- F4: Positive response for the authentication.
- F5: The CA will send the CA and end-user certificates in the MIME body to the UE. The mime body is protected using the same AKA session keys as in previous messages. Alternatively, the certificates could be identified by reference to some external directory.
- F6: Positive response from the UE.

Attribute certificates can be requested from the visited network in the following way:



The content of these messages are as follows:

- F1: SIP MESSAGE including signed certification request for attribute certificate. The request is protected using the existing IPsec connection. The identity used in the attribute certificate may be the same, which was used in identity certificate. In that case, the identity certificate (or a reference to it) needs to be included in the request.
- F2: A response for the subscription indicating that the request has been accepted.
- F3: The CA will issue the attribute certificate and send it to the subscriber in the MIME body. Alternatively, the certificate can be identified by reference to some external directory.
- F4: The response to the message.

Even though this approach may break some principles of IETF, it does not require any additional standards from IETF. More important is that the use of the certificates follows more strictly the IETF standards.

4. Comparison

In this chapter we shortly compare some aspects of the proposal presented in [S3-020300] and the ideas of this discussion paper.

- HN vs. VN to issue certificates: In [S3-020300] the VN issues subscriber attribute certificates. This paper suggests that the HN issues subscriber identity certificates and VN may issue the attribute certificates. The HN

and subscriber have a trust relationship where subscriber's identity is verified with an ID-card. This trust is delegated with AKA to the certification process and hence identity certificates can be legally binding. Subscriber attribute certificates can be used as in [S3-020300], and if they are used in conjunction with identity certificates also the subscriber's identity can be proven to SPs.

- Proof-of-possession (PoP): [S3-020300] does not include PoP because of the limited bandwidth in signalling channel. We feel that PoP should be included not to rule out some use cases and applications for certificates. For example, the certificates issued without PoP may not be legally binding in terms of local legislation. With application layer protocols the bandwidth is not a limiting resource.

- Access independence: [S3-020300] uses a GPRS –specific signalling channel, and SGSN acts as a CA. This approach is not access independent. It effectively rules out for example subscribers using WLAN access, or other alternative accesses. The application layer approach is not limited in terms of alternative access methods.

- Network layer vs. application layer: Certificates are most often used with applications. The use of network layer for certificate protocols might cause some layer-violation problems. See [S3-020365] for further discussion.

- Protection of certificate related messages: In [S2-020300] the signalling channel is integrity protected. With an application layer protocol the messages can be protected with shared secret keys (for example IK) independent of any lower layer security. In addition to that, the interface between UE and P-CSCF can be protected with IPsec if IMS is applied.

An application layer approach can provide all the features of [S3-020300]. It is also compliant with the requirements defined by SA1 in [S1-021685]. Moreover, the application layer approach can provide some additional features , like legally binding certificates. A standard application layer approach is also a good starting point towards a global PKI.

5. Conclusions

There are many potential application layer "transport" mechanisms that can be used to request subscriber certificates. Several parallel "transport" mechanisms should be allowed in order to cover different UEs. More important would be to have a standard way of using AKA generated session keys to authenticate and integrity protect the certificate management messages between the UE and the appropriate CA.

It is suggested that SA3 takes the following as working assumptions in relation to subscriber certificates:

1. Application layer approach.
2. Home network controlled model.

It is also suggested that SA3 should study if IMS could be re-used for certificate management.

6. References

[RFC 2510]: Internet X.509 Public Key Infrastructure Certificate Management Protocols, RFC 2510.

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

[S3-020365]: Analysis of Subscriber Certificates Concept (Siemens) – SA3#24 Helsinki, Finland, July 2002

[S1-021685]: Liaison Statement on subscriber certificates (Nokia) – SA1#17 Durango, USA, August 2002