3GPP TSG SA WG3 Security — S3#26 **S3-020605**
19- 22 November 2002
Oxford, UK

Agenda Item:

Source: Nokia

Title: Comments on S3-020500 “Contribution to discussion on architecture and trust for subscriber certificates”

Document for: Discussion

Date: November 8, 2002

1. Introduction

This contribution provides comments on Siemens paper (S3-020500). We agree with many of the comments made in S3-020500. Below are some clarifications and responses. Each section in the document refers to the section with the same number in S3-020500. The original quoted text is in smaller font.

2. The need for an agreement among operators on subscriber certificates

"It is argued in [Nok1] that ... no interoperator PKI is needed."

[Nok1] (S3-020542) **does not** say that the interoperator PKI is not needed. In fact, it concludes with "...the proposed approach is a step in the eventual migration towards the interoperator PKI."

"*Possible reasons for need of standardized subscriber certificates”*:

We fully agree with this. The certificate profiles defined by WAP PKI (in "WAP Certificate and CRL Profiles, WAP-211-WAPCert) may be usable as a basis for subscriber certificate format as proposed in S3-020105. Also, note that “need of standardized subscriber certificates” is not the same as “inter-operator PKI”.

"If ... operators have to agree on formats of subscriber certificates, then ... how big step it would be to agree on ... inter-operator PKI in addition."

It is hard to estimate this accurately. What we are proposing is an intermediate step that achieves many of the same benefits quickly, but can be eventually extended to an inter-operator PKI.

"*Authentication of operator CA*: without inter-operator PKI a user has no obvious means of checking that he is talking to genuine operator’s CA."

With mutual authentication based on AKA, the user **does have** the means to check that he is talking to a genuine cellular operator's network element. Moreover, as described already in S3-020105 (February), the IK protected channel between UE and the network can be used to deliver a trusted copy of operator CA certificate to UE.

"*Possible evolution paths*:...it could be argued that a large majority of users are located in their home network most of the time and, therefore, a mechanism which will enable the use of new ...services in the home network would also be very valuable..."

We agree. However, a mechanism, which will enable the use of new services both in the home and in the visited network, would be even more valuable.

3. Revocation and short-lived certificates

Comparing checking the status of an existing certificate using OCSP and issuing a new certificate, S3-020500 says: "re-certification ... would be much more costly in terms of performance than a mere status check."

Each OCSP response has to be authenticated; so the number of computationally costly operations for a re-certification and a single OCSP request is the same. Moreover, with long-lived certificates every transaction potentially requires an OCSP check by the service provider (e.g. several times a day per subscriber). With short-lived certificates, that are issued e.g. once a day per subscriber, the need for OCSP checks is much smaller. It can even be avoided altogether in many applications: e.g., non-monetary applications, small transactions..

"No consideration is given to the solution preferred in WAP that the user receives ...only a url from which the certificate can be retrieved..."

Clarification: S3-020105 (February), which is already referred to in the S3-020500, reads on page 2, second line under Figure 1: "UE should be able to ... receive either a subscriber certificate or a URL to the certificate in reply."

4. Certificate management at the UE

“Standardization of the subscriber certificates will be very important in this viewpoint as it is advantageous to limit the amount of key pairs (and certificates) stored on the smartcard given its capacity restrictions…. Visited network issued subscriber certificates (as 1 to n relation from UE-viewpoint), will give higher space demands on the smartcards and may lead to more complex certificate management.”

Expired short-lived certificates can be automatically removed from UE and the space occupied by it returned to the free memory pool. Note that the certificates can be in the phone memory.

5. Interface status check in HLR

"It is not obvious why the definition of such an interface between CA_H and HLR would create more problems than the corresponding one between CA_S and SGSN."

It is not that one interface creates more problems than the other; it is that a new interface is needed even in the case where off-the-shelf PKI components are used. In other words, the use of off-the-shelf PKI components does not constitute a readymade solution.

"It may even make sense to co-locate CA with HLR⁄AuC, as both entities require special protection..."

We agree that this makes sense. But if co-location cannot be assumed in every network product, then this interface has to be defined.

6. Authentication vs. Authorization

"Would an extension of user profiles be needed, or could this be handled through roaming agreements?"

Both are possible. Extension of user profiles provides a per-subscriber control to the home operator. Roaming agreements provide a coarser control to the home operator.

7. Non-repudiation and resolution of disputes, trust relations

"...the BS_S will not be able to infer from the successful verification of a signature how the user should be billed. If this is true then also implies that the service operator has to trust the service provider..."

This is not true. Payment for a service through operator's phone bill implies business relationship between service domain operator and service provider. This requires an agreement that defines what types of operator-billed transactions are to be accepted by the service provider. Thus BS_S will be able to infer how the user should be billed.
The service operator **does not** have to trust the service provider.

8. Protocols

"procedure depicted in the figure remains somewhat unclear”

[Nok1] (S3-020542) did not go to the level of detail of a formal contribution because it was an input to e-mail discussion. Arrow 2 is for subscriber to retrieve or check the certificates of the SP (issued by the service operator). Arrow 4 is for subscribers to have their public keys certified based on AKA. The different protocols are mentioned as examples.

"OCSP (as in RFC 2560) does not support [path validation]”.

We fully agree. If the service domain operator has issued certificates used between UE and SP, there is no need for path validation.
This is an important point. If the traditional PKI approach is adopted as is, then service providers and UEs will have to perform OCSP for each link in a certificate chain. This implies either they have to visit multiple OCSP servers, or they have to off-load the task to some entity they trust.

9. Assumed main disadvantages of home-issued certificates using inter-operator PKI

Scalability:

"proposed use of short-lived certificates will tend to sharply increase the overall system load, no matter where the generation of certificates on the fly is performed (in the home or in the service domain), cf. section 3 above."

See section 2: OCSP response must be authenticated. Therefore overall system load is not likely to be less when long-term certificates are used along with OCSP.

Assume that a certificate is issued once a day per subscriber on the average and that the number of OCSP checks for these certificates is negligible compared to the number of certificate issues. The load is roughly the same as in a long-term certificate system, in which a certificate is used (and hence its status checked with OCSP) once a day per subscriber and the number of certificate issues is negligible as compared to the number of OCSP checks. But, its is also possible (and better for the cellular business) that a subscriber will get access to several value added services per day, in which case the load with short-lived certificates would be several times lighter than the load with long-term ones.

For a good discussion on similar issues, see the recent Peter Gutmann's paper in IEEE Computer, August 2002 (vol. 35, N. 8).

Need for new interfaces:

"A new interface may be needed in both solutions, cf. section 4 above"

We agree that a new interface is needed in both cases. Our point was that even if there is an inter-operator PKI we still need to specify a new interface, i.e.; off-the-shelf PKI components does not constitute a ready-to-use solution.

Privacy:

"Privacy concerns may arise from the long-term use of the same certificate."

Exactly. This is a reason for short-lived certificates.

"The privacy concern can only be addressed by the use of more certificates per user and time unit…"

Just using "more certificates" **does not** address privacy concerns. Unlinkability requires more *key pairs*. But every new key pair needs a certificate.

"…(the certificates being used either in parallel or in succession), which brings us back to the performance and scalability issues."

As discussed above, use of short-lived certificates does not cause any special performance and scalability issues.

In summary, AKA-based certificate issuing by service operator and short-lived certificates reduce the difficulties imposed by long certificate chains and revocation checks.

10. Factors influencing architectural choices

"Layering principles: It is very questionable whether they [certificate requests] should be realized through special signaling messages particular to the radio access network."
This is a valid point, which could be the reason to adopt one of the access-independent approaches outlined in S3-020486.

"WAP provides building blocks for obtaining subscriber certificates [WAP, section 7.3, "client registration"], but is not taken explicitly into account in [Nok2]."
Section 7.3 of WAP specification contains an example of a WMLscript with sample certificate request information. The script prompts the user for a password to authenticate the user to CA, but the mechanism for distributing passwords is not specified.
WAP WPKI specifications do not address management issues: e.g., whether a WAP certificate is tied to a cellular subscription, or how to revoke a WAP certificate when the corresponding cellular subscription is revoked. WAP WPKI as specified cannot be used for enrolment based on cellular authentication. Thus, the approach for subscriber certificates described in [Nok1] (S3-020542) complements WAP PKI.
The certificate management (e.g. registration and revocation procedures) is not in the scope of the WAP PKI specification.

"It is not clear why it is said in [Nok2] [S3-020486] that, for alternative 4, terminals would have to support protocols such as PIC, EAP, EAP AKA..."
PIC, EAP, and EAP AKA are mentioned as example ways to perform cellular authentication over an IP network and enroll subscriber's public key. Other alternatives are possible, too.

"Size of market which can be addressed: ...the fourth alternative does not seem to be limited regarding the type of users who can obtain subscriber certificates..."
This is a good point.

Conclusions

S3-020500 provided a number of useful comments on [Nok1] (S3-020542) and [Nok2] (S3-020486). Several of these comments have anticipated the later SA2 guidelines on the choice of architecture for subscriber certificates. The main question raised in S3-020500 is whether an intermediate solution as described in [Nok1] (S3-020542) is necessary, or whether it is possible to directly go to a solution based on generic PKI components.

In this contribution, we have clarified points made in [Nok1] (S3-020542) and [Nok2] (S3-020486) and answered the questions raised in S3-020500. The main conclusions can be summarised as follows:

1. off-the-shelf PKI components do not constitute a ready-to-use solution: additions (such as the CA-HSS interface) and modifications (such as the use of short-lived certificates) are necessary to adapt traditional PKI components before they can be used for subscriber certificates because of the enormous scaling issues involved.

2. the intermediate solution is not a replacement for inter-operator PKI and can work better when an inter-operator PKI becomes available.