3GPP TSG SA WG3 Security — S3#25 **S3-020500**

8 - 11 October 2002

Munich, Germany

Source: **Siemens**

Title: **Contribution to discussion on architecture and trust for subscriber certificates**

Document for: **Discussion**

Agenda Items: **T.b.d**

Abstract

This document is meant to contribute to the discussion on architectural and trust aspects of subscriber certificates, mainly by commenting on Nokia's document " Subscriber certification in cellular networks and the role of inter-operator PKI*" , with some remarks on the set of slides"* Architectural choices for Subscriber Certificates*".*

---

1. Introduction

It is assumed for the purpose of this document that subscriber certificates are useful. It is not intended here to contribute to the discussion on use cases.

Comments on "Subscriber certification in cellular networks and the role of inter-operator PKI" [Nok1]:

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

It is argued in [Nok1] that it is an advantage of the proposed solution to have the serving domain issue subscriber certificates that no inter-operator PKI is needed. Inter-operator PKIs are only of relevance, of course, for roaming users which want to access a service when away from home.

The inter-operator PKI is to provide appropriate certification paths so that certificates issued by an operator's CA can be verified by an entity which does not have the root key of that CA a priori. Such an inter-operator PKI would be provided e.g. by the CAs of operators cross-certifying each other. The inter-operator PKI is not needed, according to [Nok1], because the subscriber certificates are always issued by a CA of the same operator with which the service provider (SP) has a business relation and, consequently, the SP may be assumed to be able to verify the certificates issued by the operator's CA. While this is true this does by no means imply that every operator would be free to choose their own certificate formats and build their own PKI, and that there was no need for standardisation of subscriber certificates among operators.

Possible reasons for need for standardised subscriber certificates: Current PKI standards allow many options, and, without agreement on a particular certificate profile, resulting solutions would be incompatible even when agreement on a base standard, such as X.509v3, was reached. It could appear that such incompatibility was no problem as the SP using the certificate to verify a subscriber's signature and the CA issuing the certificate belong to the same domain. This argument would overlook, however, that, also according to [Nok1], the final goal is an inter-operator PKI, and different

formats would make a future evolution to such a globally interoperable PKI quite difficult. Furthermore, if subscriber certificates are not standardised the user, in general, will have no means to check the certificates he gets back from a visited CA. This may or may not be an issue, depending on the trust placed in the visited CA.

If it is true that operators have to agree on formats of subscriber certificates anyhow then one could also ask how big a step it would be to agree on cross-certificates (inter-operator PKI) in addition.

Authentication of operator CA: Without a standardised inter-operator PKI, a user has no obvious means of checking that he is talking to a genuine operator's CA. The protocol for certificate requests would have to provide such a means. This is not mentioned in [Nok1].

Possible evolution paths: the solution proposed in [Nok1] to have the service domain issue the subscriber certificates would allow the deployment of subscriber certificates before an inter-operator PKI was in place. The same would be true, however, for subscriber certificates issued by the home. While it is obvious that this would not allow roaming 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 would enable the use of new value added services in the home network would also be very valuable as a starting point, provided it did not preclude future enhancements to a globally usable mechanism. An intermediate step towards a full inter-operator PKI could be provided by limited PKIs among groups of operators with strong business relationships. In this way, there would be a certain similarity to the evolution of GPRS roaming. This comparison is meaningful in our context as some of the proposed solutions depend on the use of GPRS to obtain certificates and to obtain service. The pros and cons of the two evolution paths should be discussed further.

3. Revocation and short-lived certificates

It is argued in [Nok1] that revocation lists and status checking via OCSP would not work. In the case of OCSP the high load is mentioned with which current OCSP servers would not be able to cope. Instead, short-lived certificates are advocated. It appears, however, that re-certification, the generation of new certificates on the same public key with an updated lifetime, would be much more costly in terms of performance than a mere status check. Also, for the overall system load it does not matter whether the short-lived certificates are generated in the home or in the service domain. Furthermore, it seems to be taken for granted that the certificate is sent from the CA to the user, and, when used for service access, from the user to the service provider. No consideration is given to the solution preferred in WAP that the user receives from the CA only a url from which the certificate can be retrieved, and the user sends the url to the service provider who will use it to fetch the subscriber certificate. This model could help in easing revocation problems considerably: a revoked certificate would simply be withdrawn from the certificate repository.

4. Certificate management at the UE

The analysis of [Nok1] has been performed network-centric. A major component of our mobile environment is the smartcard that will need major functional additions for providing key pair generation and certificate management functions. Standardisation 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. Home network issued subscriber certificates (which could be a 1 to 1 relation, depending on the policy), naturally contribute in limiting the amount of needed storage for this purpose. 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.

5. Interface for status check in HLR

It is mentioned as a disadvantage of subscriber certificates issues by the home operator that an interface would be needed between the home CA and the HLR for status checking. While this is true it is open whether such an interface could be proprietary or would have to be standardised. A similar interface is needed for the solution preferred in [Nok1] between the service domain CA and the "authenticator" (which would be the SGSN in the earlier proposal in S3-020105). 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.

Furthermore, it may even make sense to co-locate a CA with a HLR/AuC, as both entities require special protection, as they store and handle sensitive data.

6. Authentication vs. Authorisation

It is proposed to bootstrap the provision of subscriber certificates by the 3G AKA protocol. But this protocol only provides authentication, authorisation is provided by user profiles. These user profiles currently do not seem to imply anything in particular about the use of value added services. How would the visited operator know whether the user is authorised to use certain value added services, and whether the home operator commits to paying the service operator in case of a dispute? Would an extension of the user profiles be needed, or could this handled through roaming agreements?

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

It is said in [Nok1] that the service operator domain (e.g. BS_S) should also verify signatures during the settlement phase (if there is one) and store them as evidence. The usefulness of this evidence, and the ability of the service operator to contribute to the settlement of disputes, seems limited: the meaning of the signature depends on the application protocol run between the SP and the UE. In general, 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 it then also implies that the service operator has to trust the service provider contrary to the trust assumptions made in [Nok1].

8. Protocols

The approach preferred in [Nok1] is summarised in Figure 2 (copied below for the convenience of the reader). Unfortunately, the detailed working of certificate management procedures depicted in the figure remains somewhat unclear as there is no accompanying text explaining it. In particular, it is not clear (to the authors of this document, at least) what the difference between arrows 2 and 4 is, and why four different protocols are mentioned (CMP, LDAP, OCSP, PKCS#10). Are they all needed, and how do they relate to the proposal in S3-020105 to use a special UMTS L3-signalling message?

It is mentioned at the end of section 1.5 of [Nok1] that all involved CAs should support online certificate retrieval and validation. For online validation OCSP is mentioned. Note here, that, if validation implies path validation, OCSP (as in RFC2560) does not support such functionality. Extensions for online validation are planned for OCSPv2, but it is currently unclear in the IETF PKIX group whether this will be available in the near future.

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

[Nok1] mentions as the main problems:
- scalability:
- need for new interfaces;
- privacy.

Most of these issues have already been addressed above. The comments are summarised here: the 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. A new interface may be needed in both solutions, cf. section 4 above. Privacy concerns may arise from the long-term use of the same certificate. This problem is not particular to certificates issued by the home. The privacy concern can only be addressed by the use of more certificates per user and time unit (the certificates being used either in parallel or in succession), which brings us back to the performance and scalability issues.

Comments on "Architectural choices for Subscriber Certificates" [Nok2]:

10. Factors influencing architectural choices

Issuer of subscriber certificates: one decision influencing the architecture is the question whether the subscriber certificates should be issued by the home operator or a visited operator, or possibly both. E.g. if the home operator is the

issuer then the first alternative (SGSN as authenticator) goes away. Some of the pros and cons have been discussed in this document. Further discussion, in particular on the resolution of disputes, based on input from operators, seems needed.

Layering principles: certificate requests are handled at the application layer. It is very questionable whether they should be realised through special signalling messages particular to the radio access network. This seems to go against well established design principles of a layered architecture.

Access independence: this requirement has played a very important role at least in the discussion on the IMS. It should be clarified how important this requirement is in the context of subscriber certificates. Clearly, the first three alternatives depend on particular transport technologies to access the CA. The access technology may even influence the security level: when, in alternatives 1 or 2, special L3 signalling messages are used to request certificates then these would be integrity-protected when the user is provided access via UMTS PS, but would not be integrity-protected when the user is provided access via GRPS. But a UMTS user may often have to switch to GRPS when there is no UMTS coverage in certain areas.

Availability of standardised building blocks/protocols: the design of new messages or protocols should be avoided, if possible. WAP provides building blocks for obtaining subscriber certificates [WAP, section 7.3, "client registration"], but is not taken explicitly into account in [Nok2]. The WAP model seems to fit into the fourth alternative discussed in [Nok2] where the new element would be a WAP PKI portal. It is not clear why it is said in [Nok2] that, for alternative 4, terminals would have to support protocols such as PIC, EAP, EAP AKA. It is not explained in [Nok2] or elsewhere how these protocols would be used in the context of certificate requests.

Size of market which can be addressed: the first two alternatives based on SGSN and GGSN address all GPRS users, the third alternative addresses all IMS users, whereas the fourth alternative does not seem to be limited regarding the type of users who can obtain subscriber certificates. Input from operators would be desirable to decide which market should be addressed.

Conclusions

The questions raised in this contribution need to be clarified before a decision can be taken.

References

[Nok1] "Subscriber certification in cellular networks and the role of inter-operator PKI", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, September 2002

[Nok2] "Architectural choices for Subscriber Certificates", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, October 2002

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

Annex: Figure 2 from [Nok1]