3GPP TSG SA WG3 Security — S3#26 **S3-020638**

19 – 22 November 2002

Oxford, UK

Source: **Siemens**

Title: **Issues relating to a PKI for subscriber certificates**

(Short reply to Nokia's comments on S3-020500)

Document for: **Discussion**

Agenda Item: **7.7 (Support for subscriber certificates)**

Abstract

This contribution briefly addresses issues raised by Nokia in the ongoing discussion on a PKI for subscriber certificates, namely revocation, scalability and the life-time of certificates, and non-repudiation and the resolution of disputes. The contribution also raises the question in how far these issues could and should be standardised by 3GPP.

---

1. Introduction

Nokia submitted a contribution to SA3#26 entitled "Comments on S3-020500 'Contribution to discussion on architecture and trust for subscriber certificates'". We agree with most comments in this contribution. We would like to raise only two points:

2. Scalability and the life-time of certificates

It is true that both, the production of a new (short-lived) certificate and the authentication of an OCSP response, require a signature on the server side, so the computational effort may be considered similar. In S3-020500, we raised a third possibility to address the revocation problem, in addition to producing short-lived certificates on demand and checking the status of long-lived certificates via OCSP. This third possibility consists in supplying only a url indicating the location of the subscriber certificate (a certificate repository) to the user who may forward the url to the service provider. The service provider could be assumed to have a longer-term security association with the certificate repository (e.g a TLS session or an IPsec tunnel), so that not every access by the service provider to the certificate repository (e.g. via LDAP) would necessitate the use of asymmetric cryptographic functions. Revocation of certificates would simply consist in withdrawing certificates from the repository. In this way, the overall computational effort could be considerably reduced, compared to OCSP status checks.

Of course, short-lived certificates could be required for reasons other than addressing the revocation problem, in particular for privacy reasons. But, as pointed out in Nokia's contribution, for untraceability the generation of a new key pair would be required. Trading off the cost for key-pair-generation with the requirements on privacy is a separate discussion. We just mention here that the use of a certificate repository, as described above, would not help to solve these privacy concerns, but would not stand in the way either.

3. Non-repudiation and the resolution of disputes

It was said in S3-020500: “ 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].”

Nokia provided the following comment on this: “ 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.”

Perhaps a more detailed investigation with concrete examples would be useful to decide this question, as there may be different underlying assumptions. Let us remark only one thing: it is said in Nokia’s contribution that “ This requires an agreement that defines what types of operator-billed transactions are to be accepted by the service provider ”. This is true, but it may still happen that the service provider does not honour the agreement. The service provider could submit some text to the user to be signed by the user, and this text may be agreed with and hence acceptable for the operator, but the text may be submitted in a context different from the one agreed between operator and service provider. This may mislead the user. So, we still believe that some trust is required between operator and service provider. To provide legally water-tight solutions for non-repudiation based on digital signatures seems to be a difficult issue requiring further investigations.

4. Scope of standardisation for 3GPP

In a companion contribution by Siemens to SA3#26, it is asked whether 3GPP should standardise certificate formats (profiles respectively) and an inter-operator PKI respectively. It should be discussed in SA3 in how far the issues discussed in this discussion thread, such as the life-time of certificates, revocation, and non-repudation are within the scope of a 3G standard.

Conclusions

SA3 is asked to define the scope of 3G standardisation work on subscriber certificates more precisely. If revocation issues are to be addressed by 3GPP then 3GPP is asked to consider the solution presented in section 2 of this contribution, which seems to offer efficiency gains with regard to the other solutions discussed so far. Non-repudiation should be investigated further.