3GPP TSG SA WG3 Security — S3#25 **S3-020512**

8 - 11 October 2002

Munich, Germany

Source: **Orange**
Title: **Contribution to discussion on subscriber certificates**
Document for: **Discussion**
Agenda Items: **7.7**

Introduction

This contribution follows input papers by Nokia sent on the 3GPP SA3 mailing list and discusses some of the arguments provided by Nokia.

Comments on [Nok1]

Trust issues

We believe the trust assumptions presented by Nokia are not entirely correct. Nokia presents the trust model as being entirely equivalent to the model used in the case of roaming customers for circuit calls. Basically, the home network trusts the visited network to accurately charge the customer's phone calls since the HN has no visibility on his customer's calls when in roaming.
As outlined by 3GPP SA1 in [SA1], there is a requirement that the HN can have some control on services provided in the VN. The reason is that the HN is responsible for his customers' billing, and the situation with service providers is quite different from circuit calls billed by the VN. Customers are quite aware of the extra costs linked to roaming calls because these are clearly mentioned in the contract they pass with the HN. On the contrary, services provided by Service Providers will be extremely varied and it is not possible for the HN to know beforehand whether the SP will correctly inform the customer of the service billing. This may therefore lead to numerous customer complaints, which is highly undesirable for the HN. Therefore we think that the requirement for some control of the HN on services accessed by its customers is an important one and needs to be addressed.

Inter-operator PKI

Nokia has presented a list of arguments against the use of an inter-operator PKI to provide subscriber certificates issued by the HN.

- Interface between the CA and HLR

First of all this interface would not be necessarily very complex to provide as both entities are in the HN backbone and therefore it could remain proprietary. Further more, even with a local PKI located in the VN, there is still the need to provide an interface between the CA and some network element (as pointed out in [Nok2], there are several open options to define which entity is chosen to connect the CA to, but whatever the option, a new interface has to be defined).

- Long term certificates and revocation

One argument presented by Nokia for local PKI in the VN is that it can issue short-term certificates, which do not need to be checked for revocation. It is also stated that providing revocation checks for an inter-operator PKI would be fairly complex. We think that it could still be achieved for subscriber certificates.
Small granularity of revocation is mentioned as a cause for concern. Alternative option of short-lived certificates will not offer a small granularity either. Furthermore, it could be possible to develop some message slightly similar to IST for the HN to signal the revocation of a certificate to the VN.
Performances issues were mentioned, but it seems quite unclear at the moment whether trying to perform online revocation checks will actually cost more in performance than issuing local certificates very often.

Comments on [Nok3]

In the list of use cases described in that contribution, the use case linked to location services requires a certificate from the home network. While we understand why this is needed since the location services entity is located in the HN, we do not really see how Nokia's proposal of a local PKI in the VN can address the issue. It seems to us that this use case actually outlines the problems linked to having local certificates compared to using HN issued certificates.

Conclusion

Most importantly, we would like to see the requirement for home control to be addressed in the solution that SA3 will adopt for support of subscriber certificates. Secondly, we also believe that the possibility to build an inter-operator PKI for that support should be carefully examined because in our view it provides a better solution for the purpose of the work item.

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 17th 2002

[Nok2] "Architectural choices for Subscriber Certificates", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, October 1st 2002

[Nok3] "Use cases for Subscriber Certificates", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, September 24th 2002

[SA1] "LS on Subscriber Certificates", S3-020463, liaison statement from 3GPP SA1