3GPP TSG SA WG3 Security — S3#36 **S3-040929**

23 - 26 October 2004

Shenzhen, China

Title: **explanation of PDG certificate profile**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **WLAN-IW**

1 Introduction

In SA3#35 meeting, contribution S3-040717 introduced the profile of PDG certificate. There were comments that this profile should be streamlined with NDS/AF profile.

This contribution explains the difference between the PDG certificate profile and NDS/AF profile.

2 Discussion

In S3-040717, it says:

Certificate processing requirements:

…

k) *UE may check the validity of the certificates using CRLs or OCSP. Support for CRLs and OCSP is optional.*

While in NAS/AF it uese LDAP to get CRL.

The reason of using OCSP is that it's unlikely for UEs to actually implement CRL checking. UE is quite different from NDS/AF where the gateways have plenty of memory, processing power and network bandwidth.

So there isn't problem to use different revocation mechanisms here and in NDS/AF. Currently the CR allowed CRLs (with HTTP) and OCSP, and it's much more likely that OCSP would be supported.

In S3-040717, it says:

Certificates used for authentication of the PDG shall meet the following profile of RFC 3280 [39].

…

l) The KeyUsage extension shall be present in all certificates. The keyCertSign bit shall be set in CA certificates, and digitalSignature bit shall be set in PDG certificates.

There was comment saying keyEncipherment bit shall also be set as in NDS/AF profile.

The reason of not setting keyEncipherment is that NDS/AF uses IKEv1 and the keyEncipherment bit does make sense for some authentication modes of IKEv1, while we're using IKEv2 in PDG certificate profile, where the keyEncipherment bit doesn't make any sense.

3 Conclusions

It’s reasonable to use OCSP in PDG certificate profile and the keyEncipherment bit needn’t to be set.

4 References