3GPP TSG SA WG3 Security — S3#28 **S3-030254**
6 - 9 May 2003
Berlin, Germany

Agenda Item: 7.9

Source: Alcatel

Title: Location of key pair generation

Document for: Discussion

Introduction

In reference to the new draft TS titled “Bootstrapping of application security using AKA and support for subscriber certificates”, the issue of where the public/private key pair being certified is generated has not been addressed.

This brings up issues for the protocol in question, as well as security threats, as discussed below.

Discussion

Two possibilities exist, the public/private key pair can either be generated in the UE or it can be generated outside the UE somewhere in the network (e.g. in the RA or CA). The place where the key pair is generated can put specific requirements on protocol B as follows.

1. Key pair is generated in the UE

Protocol B should be able to have the following possibilities:

- UE must be able to send a certificate request containing the public key (in the case where the UE has generated his own key pair).

Key pair generation must in this case be supported by the UE.

2. Key pair is generated in a network element outside the UE

In this case not only the certificate but also the public/private key pair must be (securely) delivered to the UE.

This puts the following extra requirements on protocol B as follows:

Protocol B should be able to have the following possibilities:

- UE must be able to send an “empty” certificate request i.e. a reuqest with no public key,
- and consequently encryption of the private key is needed for the response.

In the light of the second possibility above, it should be remembered that not all protocols have the possibility to send “empty”certificate requests and include an encrypted private key in the response.

Further, if it is possible via Protocol B to request a key pair from the CA, then this also gives a security issue when Protocol A is based on AKA. This was introduced and discussed in SA3#27 with Alcatel contribution S3-030037. It was discussed that the secure link is then between the CA and the ME, rather than between the CA and the USIM, since the decryption algorithm is implemented in the ME. The ME then needs to securely pass the received key pair to the USIM. This can pose a possible security threat.

This threat will increase as mobile terminals evolve from a rather closed, secure type of mobile phone to a more open PDA or PC type of terminal.

The threat does not exist if the key pair is generated in the USIM.

Conclusion

The place of the key pair generation can have implications on the choice of the certificate request/response protocol and on security measures that need to be taken. It should therefore be considered in the TS.

Proposal

As outlined in the discussion section above, the issue of where the public/private key pair may be generated should be addressed, and the further requirements and consequences of this.

Correspondingly, the results of this discussion should be reflected in the corresponding TS.