3GPP TSG SA WG3 Security — S3#16 **S3-000709**

28-30 November, 2000

Sophia Antipolis, France

Source: **Nokia**

Title: **Support of certificates in 3GPP security architecture**

Document for: **Discussion**

Agenda Item:

Currently, it is technically feasible to provide mobile users with new type of services, such as multimedia-over-IP, using a variety of access technologies and communication mechanisms. A major stumbling block is the lack of a large-scale infrastructure to authorize and charge users for such services. Such an infrastructure may be built from scratch. But this could take years. Alternately, by making some minor additions to the 3GPP security architecture, we can allow charging for these services to be bootstrapped over the existing authentication and billing infrastructure in cellular communication systems (hereafter referred to as the "cellular infrastructure").

We propose to do this by bootstrapping a local public key infrastructure (PKI) from the cellular infrastructure. This is different from traditional approaches to using public key technology, which, presumes a global PKI and trust infrastructure. Attempts to build such a global infrastructure has so far not succeeded. Bootstrapping a local PKI as proposed has a better chance of success.

The 3GPP authentication and key agreement process results in an integrity key IK between the user equipment (UE) and the serving network. We can use this authenticated channel to submit the user equipment's public signature verification key and obtain a temporary certificate issued by the serving network. The UE can then use its signing key to sign service requests. A service provider who knows the signature verification key of the local serving network can verify the UE's certificate and signature, and can use it as an authorization for service. Any charges resulting from the service can be added to the user's mobile phone bill.

This proposal has the following advantages:

Secure authorization and charging for new services

- does not require any per-user configuration, e.g., in subscriber databases, before a mobile user is allowed to access new services.

- does not require trusting external entities and can enable non-repudiation (since the scheme is based on public key digital signatures which are unforgeable); consequently this approach can also be an enabler for low- and medium-value mobile commerce transactions.

- is efficient (the cellular infrastructure need not be involved in every external access control decision).

To efficiently implement this proposal, we propose the following additions to the 3GPP security architecture (only the first of these additions is absolutely necessary):

- A pair of new signalling message types for "certificate request/response". The serving network element should recognize the certificate request message and route them towards the local certification authority (CA). Similarly it should recognize the certificate responses and route them towards the UE.

- To support long-term public keys, an extra 160-bit field in the *Authentication data response* of the 3GPP authentication and key agreement protocol, intended to convey a public key digest from HE/HLR to the visited network. (Short-lived public keys can be generated by the UE at any time.)