3GPP TSG SA WG3 Security — S3#17 **S3-010040**

27 February - 02 March, 2001

Gothenburg, Sweden

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. This is feasible, however the public signature verification key should be encrypted all the way to the certifying CA. This is essentially the only security window of vulnerability for this public key (prior to certification). Why? It is the integrity protection which is needed here.

The public key submission or certificate request should additionally be signed by the UE's private signing key. This is essential to ensure that the correct private key is being certified.

Can be added -> it does not complicate the procedure proposed and it provides proof of possession (POP)

How temporary is this certificate, i.e. what would be its validity period?

Not standardized anyhow.

The UE can then use its signing key to sign service requests. This is a logical approach. 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.

These are standard certificate and signature verification functions in a PKI environment.

Is the intention to use this temporary certificate simply to provide proof of intent to purchase?

No but it can be used for that also.

Is this certificate for a one off purchase or would it be re-used e.g. for subscription services?

The latter. It covers single or many purchases during the validity period. It can be used also for subscription based access control.

There may be three kinds of certificates:

- for purchases

- attribute certificate (e.g. to access some flat-rate subscription service)

- id certificate for IMSI-based access control (the Service Provider has to know the IMSI)

This does not necessarily imply there are many types of certificate requests because the information about the use type can be put into the signing procedure also.

If it is to be re-used for subscription services then it may be necessary to store this certificate on the network and to present it every time a paid for service is accessed.

This is possible but not necessary. Service could be provided by anybody (e.g. a florist).

Any charges resulting from the service can be added to the user's mobile phone bill.

Would the user's available credit not be checked before the service was provided? The inclusion of this event in the overall service request process could materially affect the point at which a certificate is issued e.g. a certificate should only be issued after purchase authorisation from the billing entity has been received.

The merchant may make an on-line check towards the operator but in his/her own risk this can be skipped (e.g. for low-value transactions with physical presence of a buyer).

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. I would expect that the lifetime of the certificate would be equal to e.g. the subscription period purchased. These "short life" certificates are usually referred to as "Attribute Certificates".

ok

Attribute certificates are "sub certificates" usually generated on the fly typically used only to authorise access to resources or services. They are usually issued to holders of an "identity public key certificate" to which they are irrevocably bound. One of the

advantages of these certificates having a short life is that they will not usually need to be revoked and will therefore not need to be included on any CRLs. They may also not require revocation if they are issued in respect of a fixed time length subscription service which has already been paid for.

Our attribute certificate is directly tied into a key (not as a sub-certificate of id-based certificate). It can also be use as id-based certificate.

- 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.”)

I presume the 160 bit field is to carry the 160 bit hash of the SHA-1 hashing algorithm. One might expect that this hash would also be signed by the UE’s private key to ensure data integrity. This would also provide authentication of origin for the hash and its associated data component.

You can do this anyhow by 160 bits on the back-bone signalling. If POP is provided over the radio i/f there hash can be signed if this is seen preferable.

Why the reference to “long term public keys” here, whereas the document only refers earlier to short term keys?

The confirmation from home increase the level of trust on the keys. Earlier we only referred to temporary CERTIFICATES (not keys). If the certificates are short-term then the keys can be short-term as well (if wanted).

How would the UE guarantee the uniqueness of the key pairs generated?

Out of scope of standard. This is a general issue not related to how to bootstrap PKI. The home operator can be involved when the keys are created ("long term keys").

Other Comment

1. The signing function should provide a good level of UE authentication and non repudiation. It will still however need the services of a traditional PKI infrastructure, such as the Certification Authority, together with the ability to check for the revocation of

certificates (e.g. the serving network) as part of a UE certificate/signature verification process.

YES but this is a local issue.

2. A sound business process would call for all certified public key components of signing key pairs to be stored in a key backup server to be able to provide historic key validation services e.g. in the event of a commercial dispute to be able to verify the signature on a past service request. This would require the storage of every signing public key certificate for a given period of time. I suspect that this would require significant secure storage facilities and management overhead for a large active user base.

   If there is no PK in the home then there is no need to store any certificates for a long time because in this case the visited operator is trusted. In the case where hash of PK is sent from home the visited network has to store one certificate (or actually a PK) for each user until the bill is paid.

   Why are 3GPP not looking at a process where the USIM is enabled with a signing key pair at personalisation time? The public key component of this key pair is certified by the CA OTA and the resulting public key certificate is placed in a directory service application. It is also stored in a key backup server. "Service Certificates" would only be issued to provide access control to a service, with restricting parameters defining type of service and length of service. The service request would be signed by the UE's private signing key. The "service certificate" would be generated and signed by the network CA. For future signature verification purposes only the public key certificate of the UE's signing key would need to be stored. Since this key would a relatively long life it would considerably reduce the key storage requirements.

   This is the ideal global PKI model. Our proposal is the first step towards this goal. We try to take the "evolutionary" path, not "revolutionary".