3GPP TSG SA WG3 Security — S3#19 **S3-010304**

3 - 6 July, 2001

Newbury, UK

Source:	**Telenor**
Title:	**A first input on the use of PKI as an authentication framework for NE authentication in NDS**
Document for:	**Information**
Agenda Item:	**7.2**

A first input on the use of PKI as an authentication framework for NE authentication in NDS

The two companion documents to this document is provided to give a first input on how PKI might be used in NDS.

They are offered now for information to SA3 and it is suggested that this issue is revisited at SA3#20.

/Geir M. Køien

Basic PKI concepts

Introduction to PKI

The advantages of public key security compared to secret key are:

- Out-of-band distribution of keys can be avoided
- Better suited for large scale deployment
- Supports establishment of secure communication between entities that are previously unknown to each other

The problem related to security between strangers is unfortunately not completely solved migrating to public key systems. Also in a public key setting it is far from obvious that a public key claimed to belong to a certain entity really does so. There is a need for an "introducer" that vouches for the binding between a public key and the identity of its owner. Such a guarantee is provided by a digital certificate. The management of digital certificates through its whole lifecycle, from initialisation through utilisation to cancellation, is what public key infrastructure – PKI, is all about.

PKI services

There is no such thing as a comprehensive or authorized list of PKI services. In literature one can find almost all kinds of security services named as PKI-services. For our purpose it will be more fruitful to narrow the list. It could provide a good start to distinguish them from the security services that is ultimate from the users perspective, namely *authentication*, *integrity* and *confidentiality*. In this context we would also prefer to regard *authorization/access control* and *non-repudiation* as belonging to this category. We suggest to regard PKI services as services *supporting* these primary security services mentioned above in a context of public key cryptography. The following table provides a suggestion for some useful PKI services (although by no means exhaustive):

Certificate issuing	Certificate validation	Certificate revocation
Key generation	Key backup	Key recovery
Secure time stamping	Cross-certification	Privilege management

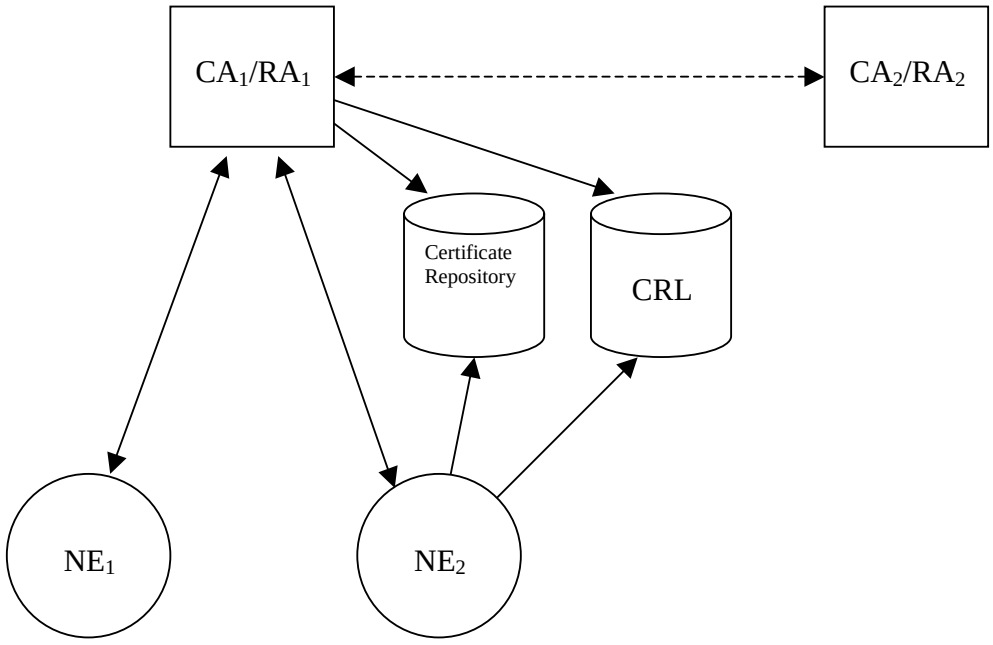
The granularity of the service definitions can always be questioned. As an example we here include several distinct steps in the handling of certificate requests in the term *certificate issuing*. It will greatly vary from application to application how comprehensive a set of services that is needed. (E.g. in applications where big transactions of money takes place, services supporting confidentiality and non-repudiation would be requisite and where sensitive medical data are transferred, services to support integrity and authorization would be desirable.) The subset of services needed in UMTS network domain security might be less than the services in the table above. Key pairs can be generated outside the PKI. In that case key backup and key recovery are neither relevant. Time stamping service might have some justification in an inter-operator scenario. Depending of the chosen PKI architecture, cross-certification might be relevant. A minimum subset of services needed in UMTS network domain security would encompass

- key generation

- key distribution
- certificate issuance
- certificate validation
- certificate revocation.

PKI architecture

In order to provide the services some entities conducting certain roles has to be in place. A Certification Authority is an entity offering the basic certification services. Among the services are issuance, validation and revocation of certificates and possibly key



generation. A Registration Authority can offload the CA with certain functions like

- establishing and confirming the identity of a new network element
- initiate the certification process on behalf of a network element
- generate keying material on behalf of a network element
- perform certain key/certificate life cycle management functions, such as to inititate a revocation request or a key recovery operation on behalf of a network element

Furthermore, there have to be publishing entities where certificates can be fetched and revocation lists can be inspected.
A simple PKI is illustrated is illustrated in figure above.

The roles of the PKI elements are:

Abbreviation	**Full name**	**Role**
NE	Network Element	Part of UMTS core network – not part of PKI

CA	Certification Authority	Responsible for issuing and revoking certificates. Possibly responsible for inter-CA relations
RA	Registration Authority	Responsible on behalf of CA for authenticating the NE on initial request for certification.
CRL	Certification Revocation List	Database maintained by CA where list of revoked certificates is published
	Certificate Repository	Database maintained by CA from which the digital certificates can be retrieved

Digital certificate

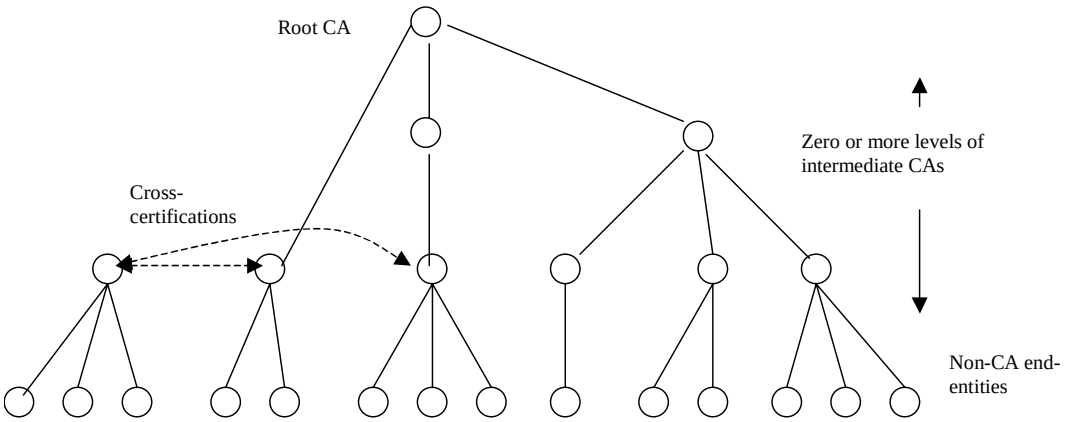
A digital certificate constitutes the means by which the relying user is assured that

- the integrity of the public key (and any other associated information) is sound
- the public key (and any other associated information) has been bound to the claimed owner in a trusted manner

Although several types of certificates exist, the X.509 is the most widely accepted standard. It has proven applicable in a wide variety of applications largely due to the flexibility in the current version 3. In X.509v3 just a smaller number of fields are always present, but it is possible to define extensions that is relevant for the application in question. These extension fields can be set as mandatory or optional. The set of fields used in a particular application of X.509v3 certificates and the mandatory/optional status of these fields constitutes a *profile*. While the X.509v3 standard is very open, a profile defines the limiting rules suitable for a particular use.

Trust relations

Two communication parties relying on a common CA can communicate securely. CAs can be organised in hierarchies, meaning that two communication parties can communicate securely also if the two CAs on which they trust is not the same but have a common root CA on top of the hierarchy. Two CAs can also be cross-certified, meaning that a digital certificate issued by one of them is acknowledged by the other and/or the other way around.



Potential use of PKI for core network security

Scope of this document

A public key infrastructure in UMTS could be deployed for two main purposes. One is to support *end user applications* and the other is to support the need for what one could call *UMTS network internal trust management*. In the latter case three areas are of interest:

1. Network access security
2. Intra-operator network domain security
3. Inter-operator network domain security

With network domain security we here primarily mean *security between network elements*. These network elements can belong to a single operator (intra-operator NDS) or they can belong to different operators (inter-operator NDS). In a broader definition the inter-operator scenario could be further extended to comprise *business relationships* concerning economic responsibilities (e.g. billing). The business aspects are considered to be out of the scope for this contribution, and so are the network access security as well as end user security.

Motivation for PKI in UMTS core network

Scalability and key distribution

So far, in proposals for core network security in UMTS based on IPsec, agreements on keys and security associations are carried out on a bilateral basis. As the number of operators and network elements increases, it would constitute a more *scalable* solution to replace individual bilateral relationships by a smaller number of multilateral agreements. The number of keys needed in a symmetric system with *n* network elements communicating with each other is n(n-1)/2, ie when n grows, the number of keys increases exponentially. In the public key case, the corresponding need for keys amounts to 2*n. So when n becomes large, the costs in terms of key generation and distribution associated with the introduction of network element *n+1* are very dissimilar in the two cases.

Dynamic key management

Authentication between network elements in UMTS Release 5 is so far planned to be based on pre-shared secrets. This is a somewhat rigid way to provide authentication. A properly designed PKI (based on digital certificates) will have more dynamic mechanisms to issue certificates for new network elements and to exclude certificates that are no longer valid. A certificate should for example be revoked if the corresponding private key is compromised or if a network element of some other reason should no longer be trusted.

More manageable trust

In TS 21.133 two requirements related to network domain security are:

- It shall be possible to secure infrastructure between operators.

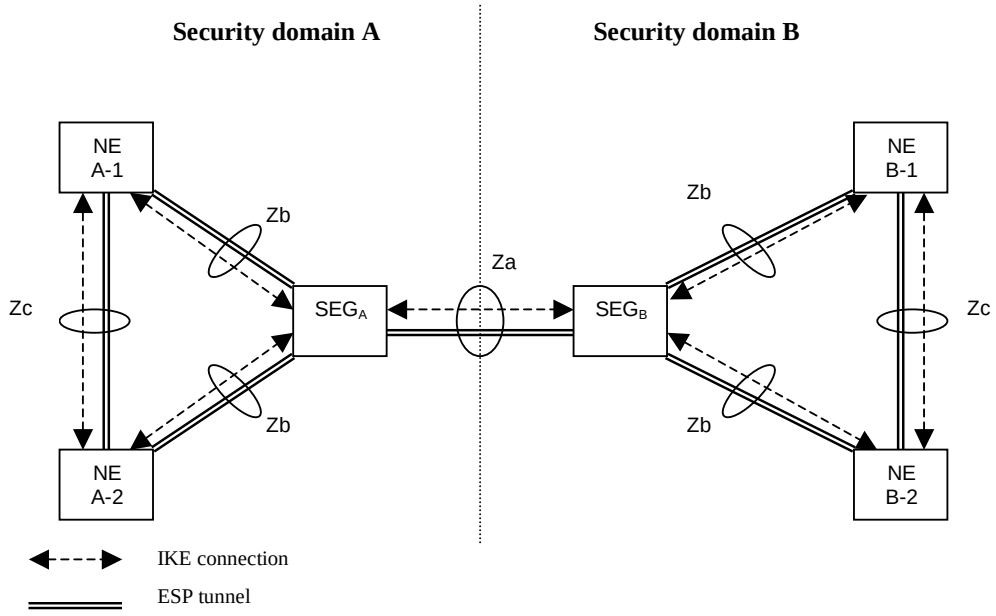
- There shall be a secure infrastructure between network operators, designed such that the need for HE trust in the SN for security functionality is minimized.

Both requirements address inter-operator security. The first requirement just states that in one way or other it should be possible to provide a secure infrastructure between operators. The second one deals with *trust relationships*.
In the first releases of UMTS the HE trust in the SN is fundamental. The AKA procedure heavily relies on the assumption that the HE can trust the SN and delegate the execution of the authentication to the SN. By introducing a commonly trusted third party the prerequisite for bilateral trust is reduced. The HE will then at least be able to authenticate the SN in a secure way. One could further consider whether a certificate for a SN network element should include information about its AKA implementation. In that case the certificate could provide the HE with confidence that the SN is trustworthy. But this would make the certificate rather application specific.

Public key shortcomings

It should be noted that secret key cryptography has its clear advantages when it comes to key lengths and computational load. Therefore public keys should not necessarily replace secret keys in all applications. The secret key regime is well suited for providing confidentiality and the public key system should primarily be used for authentication and secure transport of (symmetric) session keys.

Description



Public key infrastructure could be introduced stepwise in the UMTS core network. The order of the steps would be decided by the needs. We believe that the need for *inter-operator* trust management will be the first issue to solve. Therefore we indicate the following phases (since the CA is the most fundamental element in a PKI, we omit the other PKI elements in the brief descriptions):

Phase 1: Inter-operator NDS

- In the simplest form this is provided by one common inter-operator CA
- IKE is used for key exchange between SEGs, but based on public keys instead of pre-shared secrets

Phase 2: Intra-operator NDS

- The structure of CAs could migrate towards one CA per operator and one ore more levels of CAs above. The CA-structure could be strict hierarchic or it could be based on cross-certification between CAs from different operators
- Every network element can get its exclusive certificate
- Trust can be established on a NE-NE basis between operators (It has to be considered thoroughly whether this is desirable)
- SEGs might be superfluous in terms of providing confidentiality, but might still be needed for their firewall functionality
- IKE can in this case be used for key exchange between all network elements, but based on public keys instead of pre-shared secrets.

Phase 3: Network Access securit**y**

- Provided that an operator has his own PKI, the infrastructure could be re-used to support AKA. One reason for not choosing public key based AKA so far has been the restricted smart card performance. This restriction will be less important in the future.

To be investigated further:

The ultimate argument for introducing PKI in UMTS core network security will be its scalability properties. Therefore one has to consider thoroughly how fast the number of network elements that is sharing a security association is likely to grow. At first sight it seems probable to us that the number will be large enough to justify the public key approach.

Introduction of a PKI will probably slow down security procedures. Getting access to frequently updated certificate information (e.g. from CRLs) has the price of more latency. Therefore it has to be investigated whether PKI-introduced latency will be significant for UMTS network performance.