3GPP TSG SA WG3 Security — S3#15bis **S3z000025**

Ad-Hoc meeting 08-09 November, 2000

Munich, Germany

Source: **Motorola**

Title: **Security Services using Public Key Cryptography**

Document for: **Discussion**

Agenda Item: **TBD**

Current wireless network standards exclusively employ symmetric key methods to perform user authentication, signalling and data encryption, as well as message integrity protection. However, in current wireless applications the flow of services is from the network to each of many users. Thus, in a "one to many" communications relationship, symmetric key provides a simple but elegant architecture. The simplicity cannot be sustained, however, when the character of the trust model becomes "many to many".

Many to many trust models are better served by public key systems. The attractiveness of public key cryptography in many to many systems is partially based on the fact that it does not require a secure channel to transfer keys between two or more communication partners.

Capturing the full benefits of open channel key transfers and scaling public key methods to a large population of users requires a Public Key Infrastructure (PKI).

The purpose of this contribution is to initiate a constructive discussion about the role of PKI in IP-based network security for release 2000 and beyond.

1. PKI provides a suitable trust model for many-to-many relationship

As IP-based networks are introduced to serve a large variety of applications, complex and flexible communication relationships become established, which in turn demands a complex trust model. In numerous cases, the communication partners may not have pre-arranged security agreements. In order that two unknown partners may perform mutual authentication and establish session keys, a public key based digital signature that is supported by a public key infrastructure will generally satisfy security requirements.

An example in one of our Release 2000 work items is "Access Security for IP Based Services". A SIP proxy server may not share any symmetric key with either the UE or the HSS. Digital signature is a convenient way to authenticate the proxy server. In multiparty calls, the same mobile subscriber may issue SIP invites that must be processed by multiple CSCFs. Co-ordination of the use of a common symmetric key for authenticating the SIP invite is a daunting prospect.

2. Public Key Methods have been extensively used in existing Internet Protocols

It seems prudent that when security techniques are considered for use in the IP-based network for 3G, the security mechanisms that have been developed in IETF for Internet Protocols ought to be prime candidates.

In Release 2000 Security work item entitled "Key Management", SA3 has considered the use of IETF key establishment protocol IKE (See IETF RFC 2409) as the first tier key distribution protocol between two Key Administration Centers operating in different networks. IKE is an authenticated key agreement protocl. Digital signature is one of the methods to provide entity authentication. Therefore,

if we use IETF protocol IKE as our key management protocol with its signature property, then we will need PKI.

TLS and WTLS have been considered as candidates of security protocols to protect communications between security gateways (See previous Ericsson contribution, S3z000010). TLS demands PKI.

Another example involves the use of SIP for multimedia session initiate protocol over the Gm interface (see TR 33.800 v0.2.4, S3z000007). PGP is one of the options to be used for entity authentication and SIP message integrity protection. PGP is also used for transfering the symmetric encryption keys to provide SIP message confidentiality. PGP is public key based method, even though its trust model is different from the general PKI model. Nevertheless, compared with other security mechanisms defined for SIP, PGP is a close approximation to a desirable solution.

The AAA protocol DIAMETER has been suggested as an example (See TR33.800 v0.2.4, S3z000007) of protocols between the CSCF and the HSS. One important improvement of DIAMETER compared with another AAA protocol RADIUS is that DIAMETER offers a "strong security extension" to provide proxy server authentication. "Strong security extension" is basically a digital signature based on a public key method.

Therefore, if we will import internet security technologies, PKI will become a necessary component.

3. PKI has been introduced in wireless standards, e.g. MExE, WAP

As we mentioned before, symmetric key methods have been successfully and efficiently used to provide user authentication and message confidentiality in 2G systems. The AKA mechanism, which is also symmetric key based, has been developed for UMTS. AKA has been extensively investigated and is believed to be sound and efficient to provide UMTS access security.

The IP-Based network in Release 2000 architecture has different needs. It will serve numerous perspective applications; multimedia is one example. PKI is a natural solution to provide a flexible and simple trust model to deal with the multiple applications and the more complicated relationships.

The implementation of public key algorithms in user terminals had been considered to be resource-intensive. However, the increased processing requirements of IP-capable terminals has driven the trend towards high-powered computational platforms becoming common in wireless devices. Furthermore, advanced standards such as MExE and WAP have also moved forward to introduce public key methods. This development reinforces the assertion that PKI has become an accepted component of standards that deal with "many to many" trust relationships.

4. PKI standards have been widely accepted

The earliest PKI standard was X.509. Its first version was published in 1988. The latest version (V3) was published in 1997. The certificate authorizes an owner's public key with associated information such as owner identity, key usage, certificate policy, alternative names, name attributes, certificate path constraints, and certificate revocation list.

The IETF working group named "pkix" transplanted X.509 to Internet environment implementation standards. Numerous RFCs provided implementation guidance from operational protocols (See RFC 2585) to managment protocols (see RFC 2510).

The PKCS #9 or further version also specified public key certificates with hard-coded attribute fields.

PKI is a mature technology with plenty of "on-shelf" implementations to serve as references.

5. Recommendations

It is recommended that Security for Multimedia Access be based on a public key method. It is further recommended that S3 consider whether a PKI Work Item be initiated as a distinct function under Release 4, or whether a PKI standard be incorporated into the existing WI for Multimedia Access.