3GPP TSG SA WG3 Security — S3#26 **S3-020612**
19- 22 November 2002
Oxford, UK

Title:	**PEAP PKI Considerations**
Source:	**Intel, Cisco, AT&T Wireless, Gemplus, Transat**
Agenda item:	**7.9~~9.6~~**
Document for:	**[Discussion]**

1 Introduction

This document helps clarify the ~~Although public key infrastructure concerns are primarily within the scope of SA3, we are bringing this contribution to SA2 to help clarify~~ PKI issues raised in the companion TDOC ~~S2~~S3-~~023413~~ 020611 on PEAP. We are interested in engaging with other SA3~~2~~ attendees who are examining operator PKI deployment issues in various contexts. For example, the DIAMETER base protocol draft [DIAMETER1] recommends use of TLS in cross-domain deployments. Operator PKI is also needed in this context, and it would be beneficial to establish a common foundation for PKI that could be used for PEAP, DIAMETER, subscriber certificates, and other uses.

In the TDOC S3~~2~~-02~~3413~~0611 contribution entitled "*Enhancing EAP/SIM and EAP/AKA Authentication with PEAP*," the following observation is made:

- *WLAN clients must be configured with an appropriate PKI trust policy so that user identities are never divulged to an untrusted authentication server and connections are not established with untrusted networks.*

This document examines PKI trust policy models for deploying PEAP in the context of EAP/SIM or EAP/AKA authentication. The primary recommendation is that a subscriber should only trust the root key of the home network operator during network authentication. With (U)SIM authentication, such a root key can be configured in a manner analogous to the configuration of other subscription-related information in the UICC. To accommodate scenarios where a new WLAN subscription needs to be established without prior configuration, we also recommend a PKI model where a trusted third party certificate authority is used to certify network operators. Trust in this certificate authority is limited to the context of establishing new subscriptions (or pay-as-you-go access).

We assume that subscriber authentication when roaming will be based on an end-to-end connection to the authentication server (AS) of the home network (HN). The PKI trust model proposed here also assumes that (U)SIM credentials or username/password are used rather than subscriber certificates. However, this in no way should be interpreted as ruling out the use of subscriber certificates in alternative deployments.

1.1 Glossary of Terms

- PKI -- Public Key Infrastructure. Protocols, services and standards supporting public key cryptography.
- Digital certificate – a certificate in electronic format used to verify the identity of the certificate's owner. The certificate is digitally signed by a certificate authority to verify its authenticity.
- Private Key – a data file storing a mathematical key known only by a single entity, used for creating digital signatures or decrypting messages previously encrypted by the sender, using the corresponding public key.
- Public Key – a data file storing a mathematical key corresponding to a private key known only by a single entity. The public key can be made publicly available. Others can use this key to verify signatures created with the corresponding private key, and to encrypt the messages or files which can then be decrypted with the corresponding private key.
- Certificate – an electronic document that associates a public key to a name or other identifying information of a specific individual or entity. A certificate is issued and digitally signed by a trusted third party or certification authority (using its private key).

- Certification Authority (CA) – a trusted authority or party that digitally signs certificates in order to validate the identity of a person or party.
- Root key – a public key of a certification authority. Ordinarily, a root key issues a self-signed certificate for its own key.

2 Establishing Initial Trust

A crucial issue in any PKI-based system is the certificate trust model. Unfortunately, the term “trust” is often used informally, as if trust were a binary decision dividing the world into the categories “known and trusted for everything” and “unknown and untrusted for anything”. It is better to understand “trust” as a contextual term where the relevant question is “trusted for what?” Trust should also be established incrementally, as evidence of trustworthiness is gathered. With these principles in mind, we first consider the problem of establishing initial trust with a previously unknown network provider.

If PEAP is used, the subscriber must be configured to trust a root key that directly or indirectly certifies the public key of the network’s AS. A naïve approach to this problem would be to adopt the current Web browser model and pre-configure the subscriber to trust some large number of independent root certificate authorities. Unfortunately, this approach severely erodes the security value of certificates, because there is usually a strong business incentive on the part of certificate-issuing authorities to issue as many certificates as possible. With independent root CAs, there is high risk of certificates being issued to untrustworthy parties.

There are two viable alternatives for establishing initial trust with a network operator. The first method is to receive a root key for the new network via some out-of-band mechanism and configure the subscriber to trust that key for network authentication. For example, a UICC card could be configured with one or more root keys. After receiving the AS certificate during PEAP part 1 on a new network, the subscriber could query the UICC card to determine if it should trust the certificate for initial subscription establishment.

The second method is to pre-configure the subscriber with the root key of a small number (preferably 1 or 2) of third-party network subscription root certificate authorities whose role is limited to certifying the root keys of legitimate network operators. The primary goal of the subscription root certificate authority should be to maintain subscriber confidence in its membership by preventing unscrupulous network operators from receiving certification.

It is important to note that certificates trusted for initial subscriptions are not trusted for ordinary network access until successful completion of a subscription process. In particular, the user identity should never be divulged based on certificates issued by the subscription root CA. The user will ordinarily preside over the subscription process and have an opportunity to examine sign-up pages and decide whether to proceed or abort the subscription process. Upon completion of the subscription process, the root key of the network operator is deemed trusted for routine network access.

3 Establishing A Connection

Once a subscriber has established an account with a network operator, the root key of that provider is trusted for ordinary network access. The account also is associated with the network provider’s realm name, subscriber ID, and subscriber credential. Each AS owned by the operator is configured with a certificate signed by its root key. When the subscriber initiates a PEAP connection, it receives the AS certificate and is able to verify that it is trusted prior to divulging its ID or credentials.

Note that even if the subscriber roams to a foreign network, there is no need for it to be configured to trust the certificate of that network’s AS. This is because the PEAP connection is made with the AS of the home realm designated in the initial identity exchange.

For user privacy, it is important that no subscriber-specific information be divulged in the initial identity exchange. If an IMSI-based NAI is used, the subscriber-specific part of the IMSI should be changed to hide the true identity. For example, if the IMSI is 234150999999999 (MCC = 234, MNC = 15), the UE should report its user identity as something like 000000000000000@15.234.WLAN.3gppnetwork.org. Once the PEAP channel is established, a second protected identity request is made, and the UE at that point should respond with the true IMSI identification (for example, 234150999999999@15.234.WLAN.3gppnetwork.org).

4 Certificate Revocation

Since few certificates are trusted in the proposed PEAP PKI model, the certificate revocation problem should be quite manageable. The certificates correspond to protected network servers, so there is relatively low risk of compromise of their private keys. Furthermore, only AS certificates associated with a subscriber's home network will be trusted for network authentication. This means that in most cases, any compromise of the private keys of foreign networks will be irrelevant to the subscriber.

5 Conclusion

The PKI model we recommend for PEAP is relatively simple, makes minimal use of third-party roots of trust, and does not require cross certification between network operators. Though Operator root keys need to be provisioned for subscribers, as ~~Since~~ client certificates are not required with PEAP, many of the problems associated with subscriber certification [Nok1, Nok2] do not need to be solved in this context. This PKI model is appropriate when PEAP is used with EAP methods based on (U)SIM or username/password credentials.

[DIAMETER1] Section 2.2 and 13.2 of IETF draft "draft-ietf-aaa-diameter-15.txt", October 2002.

[Nok1] "Subscriber certification in cellular networks and the role of inter-operator PKI", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, September 2002.

[Nok2] "Architectural choices for Subscriber Certificates", document by Nokia provided as input to discussion on 3GPP SA3 mailing list, October 2002