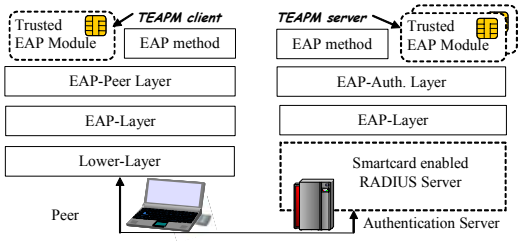
TEAPM, Trusted EAP modules.

Pr Pascal Urien, Pr Guy Pujolle.

1. Introduction.

The Extensible Authentication Protocol (EAP) is a kind of *Esperanto* used for access control in various network technologies such as Wireless LAN (Wi-Fi, WiMAX) or VPN (Virtual Private Network). In this paper we unveil the trusted EAP module (TEAPM), a tamper resistant device that securely computes the EAP protocol.

2. *What is a TEAPM ?.*



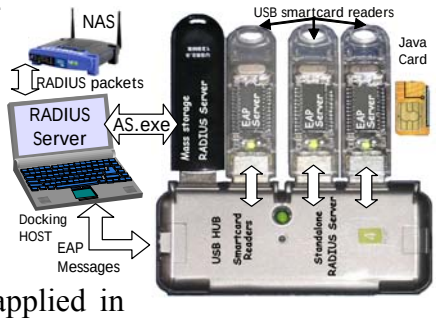
TEAPMs are smartcards that run EAP client and/or server applications. A public javacard implementation, based on the OpenEapSmartcard[1] platform is available on the WEB. Multiple client and server entities may simultaneously work in a 64 KB device.

3. Clients.

Clients work on the user's terminal and fully process standardized authentication protocols[2] such as EAP-TLS[3] or EAP-AKA[4].

4. Servers.

Servers are plugged in AAA (*Authentication Authorization Accounting*) infrastructures; as an illustration we introduce a "*smartcard enabled RADIUS server*" potentially dealing with hundreds of TEAPMs. When EAP-TLS is used, each smartcard handles an unique X509 certificate and autonomously performs an authentication session. With commercial SIM cards we observe a computing time of about 5s. However this modest performance is balanced by the parallel processing of multiple smartcards. When no TEAPM server is available, an incoming RADIUS packet is silently discarded. This mechanism is similar to the classical blocking algorithm applied in circuit-switching, where an incoming call is ignored if no output trunks are available. Under this working hypothesis, such a system follows the *Erlang-B* formula:



$$p_c = \frac{(\lambda/\mu)^c}{c!}\left[\sum_{k=0}^{c}\frac{(\lambda/\mu)^k}{k!}\right]^{-1}$$

where

- pc is the probability of blocking (e.g. a RADIUS packet is silently discarded),
- c is the number of smartcards (EAP servers),
- λ is the rate of authentication sessions, and
- 1/μ the mean time of an authentication session.

With our best couple of TEAPMs (client and server), we observe an authentication duration of about 5 + 5 = 10 s; therefore 1/μ =10. Let's assume a network with 1000 users,

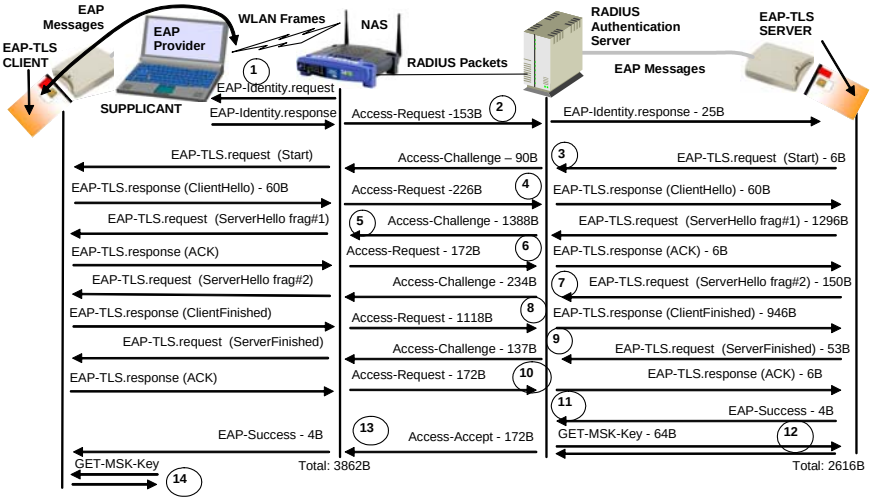
---

[1] www.enst.fr/~urien/openeapsmartcard
[2] See "OpenEapSmartCard, an open initiative for emerging open WLANs", in proceedings of eSmart'2005.
[3] RFC 2716
[4] RFC 4187

authenticated every hour, then we deduce: $\lambda = 1000 / 3600$, and $\lambda/\mu = 10 \times 1000/3600 = 2,8$. The blocking probability (p_c) is about 50% with 2 smartcards (c = 2) and only 1% with 8 smartcards (c = 8).

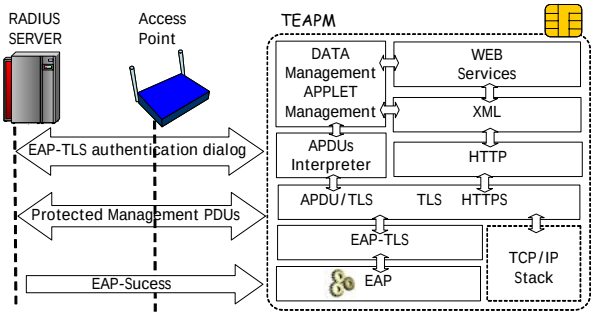
5. SAM and identity protection.

Through the deployment of TEAPMs, located both on client and server side, we re-introduce in wireless LANs, the classical paradigm of *Secure Access Module* (SAM), previously used in highly secure architecture, dealing with smartcards. Because there is a strong market requirement for privacy enforcement in WLANs, we have defined new and innovative *identity protection* mechanisms, that take advantages of unique SAM properties.



6. Remote Administration.

An other crucial property of the TEAPM, is its ability to be remotely controlled during an authentication session. Specially in a PKI context, management functions may assume the following services:



- *Cancellation of credentials*, such as X509 certificates and associated private keys. Because smartcards cloning is extremely difficult, it exists only one physical instance of these entities. The opportunity to remotely block their use, is a critical security issue in a distributed PKI environment.
- *Updating of credentials*. There is a need to guaranty continuity or extension of customer's subscriptions. This requirement is fulfilled by replacing or adding information elements, which control services availability.
- *Downloading of new applications*. Authentication protocols may evolve and include new functionalities. In that case, the software is transparently updated, e.g. without TEAPM bearers interaction.

There are several ways to tackle TEAPMs administration. First deals with legacy aspects and works with classical APDUs transported through protected TLS channels. Second uses an HTTPS transport and implies the definition of a new classes of WEB services, dedicated to smartcard management.

7. Conclusion.

As a conclusion we will underline that TEAPM technology is working in today real wireless networks. There is an unique opportunity to develop specific WEB services dealing with smartcard management.