An EAP-BT* smartcard for authentication in the next generation of wireless communications

***BT: Bluetooth**

Marc Loutrel*, Pascal Urien*, Dominique Gaïti**

** SchlumbergerSema, Smart Card Division, France, ** University of Paris VI and University of Technology of Troyes (UTT), France.*

Abstract: Wireless LANs based on the IEEE 802.11b have emerged as a new standard but still a lot of security issues remain. One of them issues is the authentication of a terminal to an access point (AP). The IEEE has released a secure architecture, IEEE 802.1x, based on the extensible authentication protocol (EAP). Similarly at the ETSI, the 3GPP has studied EAP to be used with Universal SIM (USIM) modules. In this paper, we propose an authentication architecture where smartcards play a key role.

Key words: security, smartcard, Wireless LAN, mobile telecommunications.

1. INTRODUCTION

Smartcard technology is becoming increasingly pervasive and is being adopted for a growing number of important private and public sector applications such as bank payment cards, government smartcard rollouts, mobile telephony (USIM), and E-Commerce.

[1] SchlumbergerSema, Smart Card Division, France.

[2] University of Paris VI and University of Technology of Troyes (UTT), France.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35620-4_43

D. Gaïti et al. (eds.), *Network Control and Engineering for QoS, Security and Mobility*

© IFIP International Federation for Information Processing 2003

Particularly, it is clear that smartcards will constitute a significant component of most I.T. systems in the future.

Pervasive computing exists in wireless networks like IEEE 802.11 or Bluetooth where numbers of security problems have been pointed out and need to be solved. In the first part of this paper we will describe the reader smartcard characteristics. In the second part, we will present the authentication issues for Wireless LAN and for the 3rd generation of mobile telecommunications. At last, we will introduce a new authentication architecture for the next generation of wireless communications.

2. A TAMPER RESISTANT DEVICE

A smartcard contains all the physical elements of a classic computer i.e. a microprocessor, a ROM (Read Only Memory), a RAM (Read Access Memory), a persistent memory also called E2PROM (Electrically Erasable Only Memory), a communication bus, storage ability and a way to communicate with the outside world via an I/O connector. The CPU of current smartcards is an 8-bit microprocessor with a processing power of 1 to 3 MIPS at a frequency of 3.3MHz. The new generation of RISC 32-bit (1 Million transistors) microprocessors offers a computation ability of 30Mips at a frequency of 33MHz and needs 50μs to process a DES algorithm. Only 200ms are necessary to compute a 1,024-bit RSA signature. As mentioned in [1] crypto-coprocessors may be replaced by dedicated cryptographic instruction in CPU cores. Memory capacities range from 128 to 256Ko of ROM, from 64 to 128Ko of E2PROM and from 4 to 8Ko of RAM. Writing data in E2PROM is relatively slow. It takes 1ms to write a 32 or a 64-byte word and it can be done only a million of time.

The performance of smartcards' components will be a key issue in a close future, as it will allow smartcards to be considered as the most secure communicating object on the Internet or to be limited to more classical applications.

Fortunately this will evolve rapidly. Smartcards with memories of few Mo have been announced for 2002-2003. Access to those memories is also a problem that will no longer exist with new memories such as FeRAM (10^9 writing operations allowed, memory capacity around one Mo and writing delay less than 200ns). Processors frequency will progress according to the Moore law.

Smartcards aren't delivered yet with the basics I/O interfaces (keyboard and screen) and a built-in power supply. Instead they require a CAD (Card Acceptance Device) in order to work.

Communication between a CAD and a smartcard has been defined in the ISO 7816 and offers a maximum data rate of 230400 baud in a half duplex mode through a serial link but most chips work at the speed of 9600 baud. A direct connection is provided between the new type of SPOM and the terminal via an USB port [2]. Mostly due to the APDU paradigm, physical communications have great limitations that tend to be solved according to table 1.

	Currently used by smart cards	Available in labs	Under development
Memories	EEPROM, SRAM, ROM	FLASH	FRAM
Cores	8-bit, 16-bit, 32-bit		
Coprocessors	Cryptographic	DSP, Baseband, MPEG	
Input/Output	ISO7816, ISO14443, USB, I^2C, LPC	SPI High Speed, IEEE1284, Bluetooth, Ethernet	

TABLE 1. EVOLUTION OF SMARTCARDS PERFORMANCE.

PC and PDAs are well known to be untrusted and spoofable terminals. This gives a very good reason to store sensitive information on smartcards but still we encounter number of problems. One of these problems is a PC stealing the private key off the smartcard. This is unthinkable as the attacker will be able to legally represent you by digital signature. The terminal problem described above would be solved if a screen and a keyboard were integrated onto the card bringing smartcards to the rank of a full-fledge computer. Indeed smartcards have a major role to play in terms of security in a pervasive computing environment characterized by wireless networking. Smartcards are the most secure I.T. device to store secrets information so it is now quite obvious that smartcards will be used as a secure communicating objects in the future wireless network architecture.

Some scientists are already working on Radio Frequency Identification (RFID) and the integration of smartcards in pervasive computing environment [3,4]. Figure 1 illustrates the evolution in the use of smartcards.

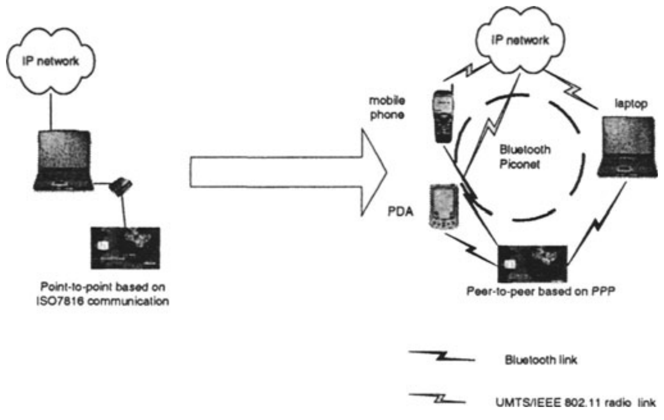
IP network
Point-to-point based on ISO7816 communication
IP network
mobile phone
laptop
Bluetooth Piconet
PDA
Peer-to-peer based on PPP
Bluetooth link
UMTS/IEEE 802.11 radio link

Figure 1. Evolution of the smart card communication model

Heterogeneous devices characterize pervasive computing environment so profiling has become another key issue. Considering this perspective, smartcards have again an active role to play. It has already been demonstrated that smartcards can be used for service accessibility and application adaptability [5].

The main quality of smartcards is to be tamper resistant, i.e. resistant to attacks whose purpose is to read all or part of the data (e.g. cryptographic algorithm keys) stored in the E2PROM.

3. AUTHENTICATION IN WLAN AND IN UMTS

3.1 Authentication in WLAN

3.1.1 Overview

In the current Wireless LAN security, two mechanisms have been defined. Access control is provided through a service set identifiers (SSIDs) and privacy is ensured through an optional encryption scheme or wired equivalent privacy (WEP).

The access control prevents unauthorized access. The terminal that hasn't a correct WEP key cannot gain access to the network. Privacy protects data streams on wireless LAN by encrypting them and allowing decryption only with the correct WEP keys.

A terminal cannot participate in a Wireless LAN until that terminal has been previously authenticated. Two types of authentication methods have been defined in 802.11b: open and shared keys.

In open authentication, the authentication process is done in clear-text, and a terminal may associate with an access point even without supplying the correct WEP key. In shared-key authentication, the access point sends the terminal a challenge text packet that the terminal must encrypt with the correct WEP key and returns to the access point.

3.1.2 Flaws design in IEEE 802.11

It is common to assign a static WEP key to a terminal. As a result, the owner of a terminal has possession of the terminal's MAC address and WEP key and can use those components to gain access to the Wireless LAN. If multiple users share a terminal, then these users effectively share the MAC address and WEP key [6, 7].

If a terminal is lost or stolen, the intended user or users of the terminal do no have longer access to the MAC address or WEP key, and an unintended user does.

The shared key authentication scheme employs one-way, not mutual authentication. An access point authenticates a user, but the reverse is not possible. If a rogue access point is placed on a Wireless LAN, denial-of-service attacks may be launched through "hijacking" of legitimate users.

WEP supports per-packet encryption but not per-packet authentication. A hacker can reconstruct a data stream from responses to a known data packet and then can spoof packets.

3.1.3 IEEE 802.1x

IEEE 802 LAN are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through already attached equipment. In such environments, it is desirable to restrict access to the services offered by the LAN to users and devices that are allowed to make use of these services. Port based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a mean of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics.

In this context, a port is a single point of attachment to the LAN infrastructure. The use of port authentication includes associations between stations and access points in IEEE 802.11 Wireless LANs.

IEEE 802.1X [8] defines the encapsulation techniques that shall be used in order to carry EAP packets between Supplicant Port Access Entities (PAEs) and Authenticator PAEs in a LAN environment. The encapsulation is known as EAP over LANs, or EAPOL and is illustrated in figure 2.

In 802.1X, the Authenticator requires the Supplicant to be authenticated before establishing the connection. This entity is typically a bridge or an access point. Basically the Supplicant is a terminal being authenticated by the Authenticator and desires access to the services of the Authenticator. The PAE is the protocol entity associated with a port therefore it can support the protocol functionality associated with the Authenticator, the Supplicant or both. Most authentication servers currently deployed are RADIUS servers.

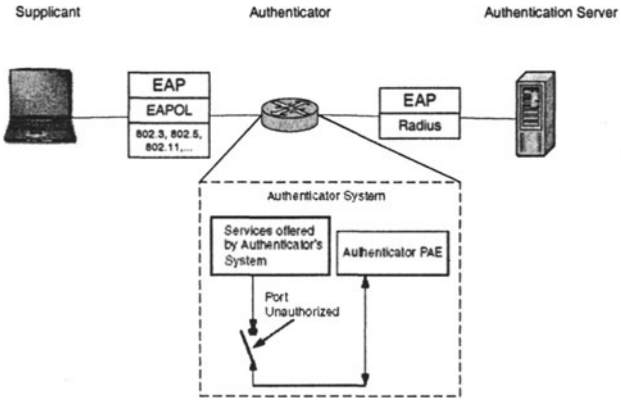

Figure 2. Authenticator, Supplicant and Authentication Server roles

Nevertheless session hijacking and man-in-the-middle are two flaws in the design of 802.1X that have already been identified and operationally verified [9].

3.1.4 Solution

The first step could be a Wireless LAN authentication based on device-independent items such as usernames and passwords, which users possess and use regardless of the terminals on which they operate. Mutual authentication between the terminal and an authentication server will prove to both sides their legitimacy within a reasonable time. The access point must support mutual authentication in order to detect and isolate rogue access points.

A WLAN security scheme should also use WEP keys that are generated dynamically upon user authentication, not static keys that are physically associated to a terminal and should support session-based WEP keys.

3.2 Authentication in UMTS

3.2.1 Overview

As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service (circuit switch for voice and packet switch for data) domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. User identity confidentiality, user location confidentiality and user untraceability are achieved by identifying the user with a temporary identity by which he is known by the visited serving network.

To avoid user traceability, which may lead to compromising user identity confidentiality, the user should not be identified for a long period of time by means of the same temporary identity. Additionally, it is required that any signaling or user data that might reveal the user's identity is ciphered on the radio access link.

3.2.2 USIM Authentication and Key Agreement

During the authentication [10], the USIM verifies the freshness of the authentication vector that is used. The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt of RAND and AUTN the USIM first computes the anonymity key $AK = f5_K$ (RAND) and retrieves the sequence number $SQN = (SQN \oplus AK) \oplus AK$. Next the USIM computes $XMAC = f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends user authentication reject back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. Next the USIM verifies that the received sequence number SQN is in the correct range. If the USIM considers the sequence number to be not in the correct range, it sends synchronization failure back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

If no failure has been reported, the USIM produces a response RES, which is sent, back to the VLR/SGSN and also computes CK and IK. The UMTS authentication process is illustrated in figure 3.

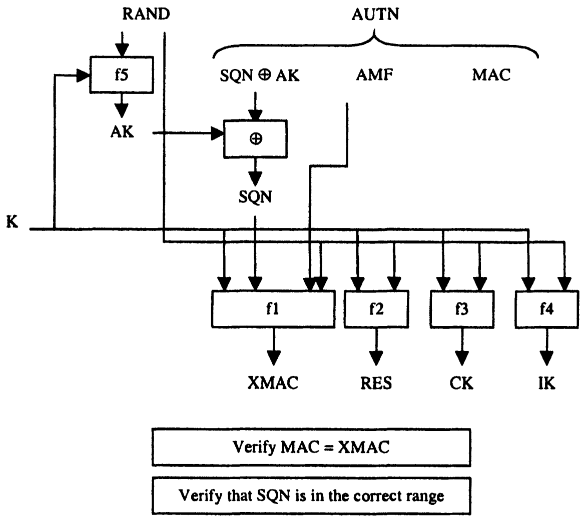

Figure 3. User authentication function in the USIM

4. EAP

4.1 Overview

The Extensible Authentication Protocol (EAP) [11] is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smartcards. As mentioned above, IEEE 802.1x specifies how EAP should be encapsulated in LAN frames. The EAP protocol can support multiple authentication mechanisms without having to pre-negotiate a particular one. A network access server so-called NAS do not necessarily have to understand each request type and may be able to simply act as a pass through agent for a "back-end" server on a host. The device only need look for the success/failure code to terminate the authentication phase.

4.2 EAP for SIM smartcards

EAP is a general protocol for PPP authentication [20]. Even though EAP was originally developed as a link layer protocol but it can be applied at higher layer too.

EAP packets include all relevant information about the required authentication scheme, packet type (request, response, success or failure) and/or challenge.

The progression of an authentication procedure depends also on the chosen authentication mechanism. Typically, the authenticator sends an initial Identity Request followed by one or more Requests for authentication information. The peer sends a Response packet in reply to each Request. As with the Request packet, the response packet contains a type field, which corresponds to the type field of the Request. The authenticator ends the authentication phase with a Success or Failure packet.

Some access point vendors to improve WLAN security already use EAP/TLS [12]. SSL was the basis for TLS protocol standard developed by the IETF. It has been demonstrated that smartcards can embed SSL so smartcards could be easily use to authenticate a terminal in a Wireless LAN.

We recently introduced [13] a new type of smartcards for authentication in Wireless LAN based on SIM-IP modules. As EAP has emerged as a standard layer to support various authentication protocols, our idea is to integrate EAP in SIM-IP smartcards.

5. OUR SOLUTION

5.1 Architecture

In figure 4, we introduce a new architecture for authentication in mobile communication.

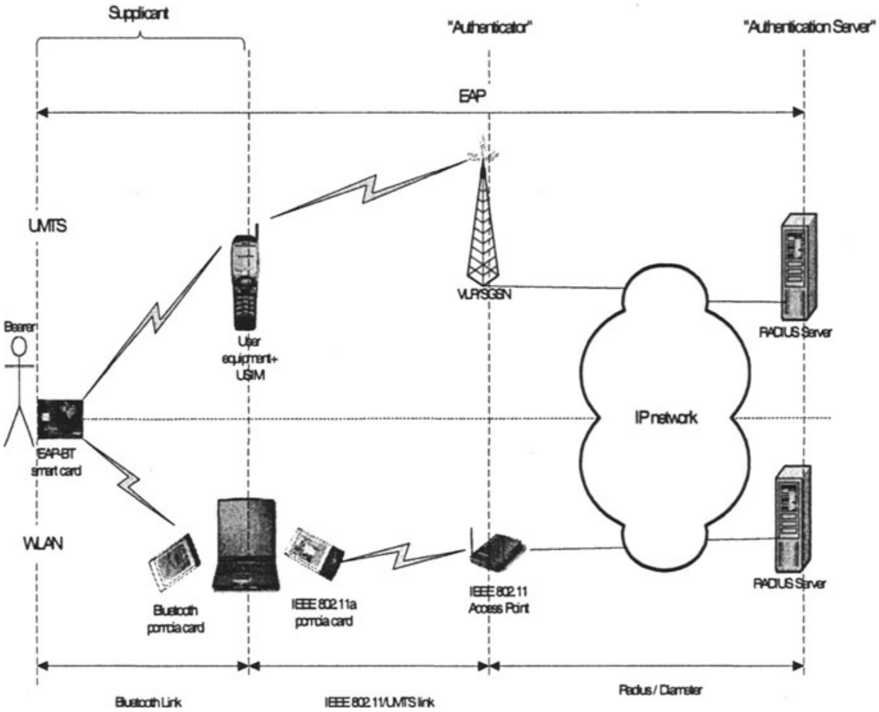

Figure 4. Authentication architecture for wireless communications.

5.2 EAP Internet smartcard

An Internet smartcard is made of four main layers as shown in figure 5:

- ***A communication stack:*** distributed between smartcard and terminal. Thanks to this entity embedded applications exchange data with remote Internet nodes. This stack is based on SmartTP protocol [14, 15], which is the only one that supports client and server applications in today 8-bit smartcards.
- ***A web server:*** manages the HTTP protocol. All smartcard resources are identified by URLs (http://127.0.0.1:8080/DES?Key1=69DA379EF99580A8 returns the ciphered value of an 8-byte number 69DA379EF99580A8 according to a DES algorithm using *Key1* key).
- ***An XML script parser [16]:*** is the central point of our Internet smartcard. It has access to every embedded resource and manages one or two Internet sessions.
- ***A file System Interface:*** manages files operations (reading, writing) and is in charge of all authentication procedures.

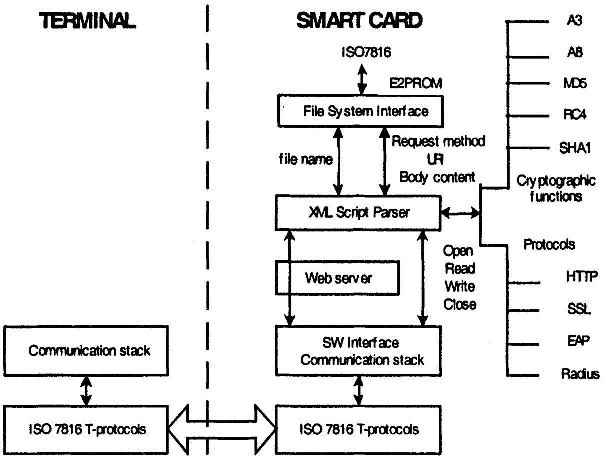

Figure 5. Organization of an Internet smart card.

5.3 Bluetooth smartcard

Bluetooth technology enables many new usages often referred as hidden computing or unconscious connectivity. On top of the data link layer, RFCOMM and network level protocols provide different communications abstractions. RFCOMM provides serial cable emulation using a subset of the ETSI GSM 07.10 standard. In a first step, a smartcard will communicate through the serial link of a smartcard reader, and in the future we expect to be able to communicate directly with a Bluetooth interface integrated in smartcards. Consequently it will be possible to integrate smartcards in a Bluetooth piconet.

Currently IEEE 802.11b and Bluetooth both operate in the unlicensed 2.4 GHz band. This may cause a problem of interoperability that will no longer exist as the IEEE 802.11a operates in the 5 GHz band. IEEE 802.11a offers greater throughput and hopefully a better security scheme in order to be widely and quickly adopted in corporate LANs.

We plan studying the Bluetooth security specification in more detail. This has to be done to ensure that our smartcard is a highly secure Bluetooth node. Also, the recent need for quality of service (QoS) in IP networks gives us another opportunity to integrate smartcards in IP networks. According to that consideration, during the MMQoS project [17], we expect to support QoS negotiation protocols in smartcards. At last, interacting in a pervasive environment brings us a new dilemma. In a pervasive environment, a user needs to access services seamlessly. Access to those services need a strong security scheme. For this reason, we suggest to use an Internet smartcard as the ultimate and secure communicated object.

6. CONCLUSION

Mobile networks are easily breakable compared to wired networks. Attacks cost to the American and Canadians industries millions of dollars. Our architecture is an attempt to minimize the fraud in the next generation of wireless networks and mobile telecommunications.

We have shown that smartcards can be the heart of the authentication scheme not only in the 3rd generation mobile telecommunications, where they have been chosen, but also in Wireless LAN.

7. BIBLIOGRAPHY

[1] Jean-François Dhem and Nathalie Feyt, "Hardware and software symbiosis helps smart card evolution", IEEE Micro p14-25, November/December 2001.

[2] SchlumbergerSema, e-gate, http://www.1.slb.com/smartcards/news/01/sct_egate1505.html.

[3] Ken Sakamura and Noboru Koshizuka, "The eTRON wide-area distributed architecture for e-commerce", IEEE Micro p7-12, November/December 2001.

[4] The communicating Mobile Objects Project, "Laboratoire Informatique Fondamentale de Lille" (LIFL) and Gemplus.

[5] Raphaël Marvie, Marie-Claude Pellegrini and Olivier Potonniée, "Smart cards: A system support for service accessibility from heterogeneous devices", In 9th ACM SIGOPS European Workshop, September 2000, Kolding, Denmark.

[6] William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, "Your 802.11 Wireless Network has No Clothes," In IEEE International Conference on Wireless LANs and Home Networks, Singapore, Dec 2001

[7] N. Borisov, I. Goldberg, and D. Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11", In *Proceedings of the 7th International Conference on Mobile Computing and Networking*, July 2001 in Rome Italy.

[8] IEEE 802.1X specification (IEEE Standard), http://standards.ieee.org/reading/ieee/std/lanman/802.1X-2001.pdf

[9] William A. Arbaugh, Arunesh Mishra, "An Initial Security analysis of the 802.1X standard", www.cs.umd.edu/%7Ewaa/1x.pdf .

[10] 3GPP Technical Specification, 3GPP TS 33.102 V3.7.0, December 2000.

[11] RFC 2284, "PPP Extensible Authentication Protocol (EAP)", March 1998.

[12] RFC 2716, "PPP EAP TLS Authentication Protocol", October 1999.

[13] Pascal Urien, Adel Tizraoui, Marc Loutrel, "Integrating EAP in SIM-IP smartcards", to be published at ASWN the second IEEE workshop on Applications and Services in Wireless networks, July 2002, Paris.

[14] "SmartTP, Smart Transfer Protocol", draft-urien-SmartTP-00.txt, June 2001.

[15] Pascal Urien " Internet Card, a smart card as a true Internet node", Computer Communication, volume 23, issue 17, October 2000.

[16] Pascal Urien, Hayder Saleh, Adel Tizraoui , "XML Smart cards", IEEE International Conference on Networking, ICN'01, July 11-13, 2001 - CREF, Colmar, France.

[17] MMQoS, http://www.mmqos.org.