Internet Draft   Florent Bersani
File: draft-bersani-eap-synthesis-sharedkeymethods-00.txt   France Telecom R&D
Expires: October 2004   April 2004

EAP shared key methods: a tentative synthesis of those proposed so far

Status of this Memo

Abstract

The purpose of this draft is to gives a broad picture of the existing proposed EAP methods, with a focus on shared key EAP methods. Indeed, it is the belief of the author that a standard replacement for EAP-MD5 (that is deprecated due to security reasons) is needed. By listing the existing shared key EAP methods, the goal is to gather consensus that such a multiplication of methods is detrimental and that a single methods retaining the best of the existing proposals could and should be drafted.

Table of Contents

1. Introduction

1.1 Purpose of this document

The Extensible Authentication Protocol (EAP) [EAP], provides an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as PPP [PPP] or IEEE 802 thanks to the IEEE 802.1X [IEEE 802.1X] framework., without requiring IP.

EAP supports many authentication mechanisms usually called EAP methods.

The purpose of this draft is to gives a broad picture of the existing proposed EAP methods, with a focus on shared key EAP methods.

Although this has already done before, see [EAP-METHSTAT1] and [EAP-METHSTAT2], it appeared worth doing the exercise thoroughly again with a view towards requesting the opening of a work item at IETF, namely replacing EAP-MD5.

Indeed, EAP methods have proliferated but only 4 are currently standardized - namely EAP-MD5, EAP-OTP and EAP-GTC in [EAP] and EAP-TLS in [EAP-TLS]. Due new security requirements, expressed for instance in IEEE 802 EAP Method Requirements for Wireless LANs [IEEE 802REQ], EAP-MD5 has been deprecated: it does neither provide mutual authentication nor key derivation. However, no simple shared key EAP method seems to be widely available to replace EAP-MD5.

In parallel to a proposition for such a replacement ([EAP-PSK]), a documentation effort has been undertaken (see [EAP-SKMDTEMPL]) to assess the different proposals, confirm that no standard replacement for EAP-MD5 exists and open the way for such a replacement by allowing comparison/merger of the existing related work. This document is the synthesis of this effort.

1.2 Material used for this document

This document has been elaborated thanks to:

- o The responses received to [EAP-SKMDTEMPL] that was posted March 2004 to the EAP mailing list
- o Investigation of the PPP EAP Request/Response Types registered by IANA ([IANA])
- o Investigation of the methods quoted in [EAP-METHSTAT2]

Although it is the intention of the author of this document to gather all the material relevant to EAP methods on a single location on the Internet, the readers might want to use the following URLs to

retrieve documents mentioned in this document while the aforementioned location is still under construction:

- o http://www.potaroo.net/ietf/old-ids/
- o http://www.watersprings.org/pub/id/

1.3 Organization of this document

Section 2 is devoted to briefly present and analyze each proposed shared key EAP method the author of this document is aware of.

Following this review, conclusions are drawn in section 3. After a brief review of the methods studied in section 2 for the sake of clarity to allow the impatient reader to directly jump to section 3 without reading section 2, a tentative conclusion on shared key EAP methods in general and replacement of EAP-MD5 in particular is proposed in this section, followed by miscellaneous points on alternative subjects noted while writing this document.

Section 4 is included for the sake of exhaustively and consists in a brief review of the other existing non shared key EAP methods. This review had to be done to ensure that the methods mentioned in this section were indeed not shared key methods and thus did not belong to section 2.

Within section 2 and 4, the EAP methods have been listed starting by those who have been attributed an EAP type number by IANA presented in increasing type number order, followed by those who have not, presented in alphabetical order according to their name.

The other sections are the typical ones of an Internet Draft.

1.4 Caveats

Though, the intention of this document was mainly to document the existing shared key EAP methods, the borderline between documenting and commenting upon was sometimes blurred. This was further complicated by the obvious potential bias of the author (who is himself the author of a proposed shared key EAP method, EAP-PSK). As the draft may evolve, this will be clarified (i.e. the analysis parts will be more clearly separated from the documentation ones and will be deepened). In the meanwhile, the reader is advised to differentiate in this document between facts and what may be considered opinions. Comments to help separate facts from opinions as well as to include other opinions are more than welcome!

In addition, gathering documentation and digesting it did not prove to be that simple. Hence, this document may unfortunately contain some errors. Readers are encouraged to report any error they feel

they have spotted (especially if they are authors of an EAP method and are dissatisfied with the treatment their method has received).

It was especially difficult to find out whether a method was still being developed or not as well as whether a method had been implemented. Hopefully future versions of this draft will clarify this.

Last, the reader not familiar with the Internet Draft process is reminded that this document is only (for now) the expression of the work of an individual and by no way the expression of a consensus of the community. It is however the intention of the author that this document evolve from the understanding and appreciation of a single person to the statement of the point of view of the community.

2. Review of the proposed shared key EAP methods

This section presents the different existing shared key EAP methods the author is aware of. These methods have been a priori deemed relevant for the drafting of a replacement for EAP-MD5.

2.1 EAP-MD5

Please refer to [EAP] and [EAPbis] for a description of EAP-MD5, which is thus a standardized method. This method has also been widely implemented.

EAP-MD5 must have been included in [EAPbis] for backward compatibility, since [EAPbis] clearly presents the totally insufficient security claims of this method (I am not sure it was even a good idea to include this method in [EAPbis] but this is another debate, see for instance Issue 174 of the EAP Issues List [EAPIssues]).

Apart from the issues already mentioned on EAP-MD5 and that are far enough to deprecate it (namely: no mutual authentication, no key derivation and high vulnerability to active brute-force/dictionary attacks), I'd like to raise two additional minor ones.

First, in [CHAP], the length of the challenge does not appear to be fixed ("The length of the Challenge Value depends upon the method used to generate the octets, and is independent of the hash algorithm used). My understanding is also that the response to CHAP is Hash(Identifier||Secret||Challenge) where Hash denotes a hash function. It is now well-known that it is not a good idea to calculate the response this way (see [MDx]), even though the appending the length of the message in MD5 thwarts the most trivial extension attacks.

Second, cryptographers tend to deprecate MD5 in favor of, for instance, SHA-1 because MD5 output is only 16 bytes and because collisions have been found for the MD5 compression function.

2.2 EAP-Cisco Wireless

EAP-Cisco Wireless is also known as LEAP (Lightweight EAP) which has been registered to IANA by S. Norman (Cisco).

It is an undocumented proprietary method of Cisco, that was shared by Cisco to participants in the CCX program. It has been reverse-engineered and analyzed (see [LEAP]).

EAP-Cisco Wireless is an EAP method that has been allocated EAP Type 17 by IANA.

It is a shared key method that builds on existing mechanisms (MS-CHAP). It has been found to be flawed due to cryptographic weaknesses inherited from MS-CHAP and very poor dictionary/brute-force offline attack resistance (see [LEAPVUL]).

There does not seem to be any intention to officially document EAP-Cisco Wireless or to modify it to remedy its known flaws. The plan rather seems to be to develop a new and broader EAP method (namely EAP-FAST, see section 2.10). EAP-Cisco Wireless has been implemented.

2.3 EAP-SIM

SIM stands for Subscriber Identity Module (it is a concept imported from the GSM world).

It is an EAP method proposed by H. Haverinen (Nokia) and J. Salowey (Cisco).

The first version of it was proposed in February 2001 as an individual Internet-Draft: draft-haverinen-pppext-eap-sim-00.txt. Version 01 published April 2001, Version 02 published November 2001, Version 03 published February 2002, Version 04 published June 2002, Version 05 published June 2002, Version 06 published October 2002, Version 07 published November 2002, Version 08 published December 2002, Version 09 published January 2003, Version 10 published February 2003, Version 11 published June 2003 and Version 12 published October 2003 are still to be found on the Internet.

It is an EAP method based on symmetric cryptography that reuses the GSM authentication infrastructure. Although it could be used without a SIM (e.g. with a software virtual SIM) and therefore as a generic shared key EAP method, it is my opinion that doing would not be appropriate since EAP-SIM makes considerable effort to deal with the

limitation of the GSM authentication (e.g. 64 bit keys or unilateral authentication). In case, one would however want to reuse such a method as a generic shared key method, I suggest at least not considering EAP-SIM but only EAP-AKA, which reuses the much more evolved UMTS authentication scheme.

Regarding IPR, some IPR claims seem to be related to EAP-SIM, please refer to:

- http://www.ietf.org/ietf/IPR/NOKIA-draft-haverinen-pppext-eap-sim.txt
- http://www.ietf.org/ietf/IPR/NOKIA-EAP.txt
- http://www.ietf.org/ietf/IPR/nokia-ipr-draft-haverinen-pppext-eap-sim.txt

EAP-SIM is an EAP method that has been allocated EAP Type 18 by IANA (under the name Nokia IP smart card authentication).

EAP-SIM is quite mature and still being actively developed. It has also been implemented. It is backed by the GSM and UMTS world (for instance by the 3GPP and the GSMA).

2.4 SRP-SHA1

SRP stands for secure remote password, which refers to a protocol developed by Thomas Wu [SRP].

It is an EAP method proposed by J. Carlson (Sun Microsystems), B. Aboba (Microsoft) and H. Haverinen (Nokia).

The first version of it was proposed in December 2000 as a PPPEXT WG Internet-Draft: draft-ietf-pppext-eap-srp-00.txt.

Version 01 published March 2001, version 02 published June 2001 and version 03 published July 2001 are still to be found on the Internet. Hints to a version 04 may be found on the Internet but I did not manage to find the corresponding draft.

It is an EAP method based on symmetric cryptography and asymmetric key cryptography to provide strong password only authenticated key exchange. This method is quite similar to EAP-SPEKE, please refer to section 2.9 for a discussion.

Regarding IPR, some IPR claims seem to be related to SRP, please refer to:

- http://www.ietf.org/ietf/IPR/LUCENT-SRP
- http://www.ietf.org/ietf/IPR/PHOENIX-SRP-RFC2945.txt
- http://www.ietf.org/ietf/IPR/WU-SRP

SRP-SHA1 is an EAP method that has been allocated EAP Type 19 and 20 by IANA.

It is unclear whether this method is still being developed or not. According to [EAP-METHSTAT1], part of this method is claimed to have been implemented.

2.5 EAP-AKA

AKA stands for Authentication and Key Agreement (it is a concept imported from the UMTS world). Where the GSM world uses the SIM, the UMTS world uses the USIM which stands for UMTS SIM.

It is an EAP method proposed by J. Arkko (Ericsson) and H. Haverinen (Nokia).

The first version of it was proposed in May 2001 as an individual Internet-Draft: draft-arkko-pppext-eap-aka-00.txt. Version 01 published November 2001, Version 03 published February 2002, Version 04 published June 2002, Version 05 published October 2002, Version 06 published November 2002, Version 07 published December 2002, Version 08 published January 2003, Version 09 published February 2003, Version 10 published June 2003 and Version 11 published October 2003 are still to be found on the Internet. I did not manage to find the Version 02 on the Internet.

It is an EAP method based on symmetric cryptography that reuses the UMTS authentication infrastructure. Although it could be used without an USIM (e.g. with a software virtual USIM) and therefore as a generic shared key EAP method, it is my opinion that doing would not be most appropriate. However, in the case of EAP-AKA, I must confess that this opinion is rather a matter of taste, regarding for instance its potential complexity and its design compared to the ones of a standalone shared key EAP method. Further technical and scientific investigation is needed to confirm or infirm this opinion.

Regarding IPR, an IPR claim seems to be related to EAP-AKA, please refer to:

o http://www.ietf.org/ietf/IPR/NOKIA-EAP.txt

Though I am not a lawyer, it seems that this claim does not really encumber EAP-AKA.

EAP-SIM is quite mature and still being actively developed. It is unclear whether it has been implemented. It is backed by the GSM and UMTS world (for instance by the 3GPP and the GSMA).

2.6 MS-EAP-Authentication

MS stands for Microsoft.

It is an EAP method proposed by Vivek Kamath and Ashwin Palekar (Microsoft).

The first version of it was proposed in September 2002 as an individual Internet-Draft: draft-kamath-pppext-eap-mschapv2-00.txt.

Hints to a version 01 may be found on the Internet but I did not manage to find the corresponding draft.

It is an EAP method based on symmetric cryptography that reuses the MS-CHAPv2 authentication protocol. It therefore bears the well-known security flaws of the MS-CHAPv2 protocol, see [MSCHAPVUL]. An interesting feature is though the password aging and changing process.

MS-EAP-Authentication is an EAP method that has been allocated EAP Type 26 by IANA.

This method does not seem to be any more under development, although it would require some, at least to comply to the [EAPbis] and [EKMF]. It has been implemented on Microsoft platforms.

2.7 EAP MSCHAP-V2

It is an EAP method proposed by D. Potter and J. Zamick (Cisco).

The first version of it was proposed in January 2002 as an individual Internet-Draft: draft-dpotter-pppext-eap-mschap-00.txt.

Hints to a version 01 may be found on the Internet but I did not manage to find the corresponding draft.

It is an EAP method based on symmetric cryptography that reuses the MS-CHAPv2 authentication protocol. It therefore bears the well-known security flaws of the MS-CHAPv2 protocol, see [MSCHAPVUL]. This method resembles very closely MS-EAP-Authentication.

EAP MSCHAP-V2 is an EAP method that has been allocated EAP Type 29 by IANA.

This method does not seem to be any more under development, although it would require some, at least to comply to the [EAPbis] and [EKMF]. It is unclear whether it has been implemented.

2.8 EAP-HTTP Digest

EAP-HTTP Digest is an EAP method that has been registered to IANA by O. Tavakoli (Funk Software).

It is an undocumented EAP method, though some elements were kindly provided by [EAPHTTPDigest].

EAP-HTTP Digest is an EAP method that has been allocated EAP Type 38 by IANA.

EAP-HTTP Digest is a shared key method that allows HTTP Digest authentication (defined in [HTTP-Digest]) to be offloaded from a gateway to an AAA server. It is applicable for use with HTTP servers as well as other protocols that use HTTP as a transport and require HTTP digest authentication (e.g. SIP).

This protocol is not intended to be a shared key EAP method that replaces EAP-MD5 Challenge, as per [EAPHTTPDigest]. It is rather driven by legacy requirements (the definition of an authentication method for HTTP that is not compatible with any existing RADIUS credentials or EAP types).

It is unclear whether this method will be publicly specified and whether it is implemented or not.

2.9 EAP-SPEKE

SPEKE stands for simple password exponential key exchange.

It is an EAP method proposed by D. Jablon (Phoenix Technologies). The actual EAP method was, as far as I know, never described. Hence, the following text only alludes to the SPEKE scheme by itself.

The first version of it was proposed in February 2002 as an individual Internet-Draft: draft-jablon-speke-00.txt.

Version 01 published April 2002 and version 02 published October 2002 are still to be found on the Internet.

It is an EAP method based on symmetric cryptography and asymmetric key cryptography to provide strong password only authenticated key exchange.

This method is quite similar to EAP-SRP.

From a security point of view, this method seems to definitely have a better security level than EAP-PSK when a password is used because it uses techniques specially designed to sophisticatedly deal with

passwords (better than the classic tips provided in the Annex B of [EAP-PSK], which are salting and iterating a hash function). A simple presentation related to the more evolved techniques to deal with password is available at [SRPpres].

It would be interesting to investigate whether this increased security level has some concrete impact on realistic usage scenarios and whether it is necessary to provide such a strong password support. The reasons why EAP-PSK did not choose to try and provide strong password authentication in a similar way to SPEKE and SRP are:

- EAP-PSK wanted to rely on a single cryptographic primitive (AES) whereas SPEKE or SRP have to use asymmetric cryptography
- EAP-PSK wanted to avoid any patent-encumbrance whereas SPEKE and SRP seem to require clarification regarding their IPR status
- EAP-PSK left totally open the way the PSK would be stored (in a human brain, in hardware or software containers,...)
- EAP-PSK felt that it could provide a decent level of security to users that chose "reasonable" passwords (this point is of course to be investigated, justified and clarified).

Regarding IPR, some IPR claims seem to be related to SPEKE, please refer to:

- http://www.ietf.org/ietf/IPR/PHOENIX-SRP-RFC2945.txt

EAP-SPEKE is an EAP method that has been allocated EAP Type 41 by IANA.

It is unclear whether this method will be publicly specified and whether it is implemented or not.

2.10 EAP-FAST

EAP-FAST stands for Flexible Authentication via Secure Tunneling (EAP-FAST).

It is an EAP method proposed by N.Cam-Winget, D. McGrew, J. Salowey and H.Zhou (Cisco).

The first version of it was proposed in February 2004 as an individual Internet-Draft: draft-cam-winget-eap-fast-00.txt.

It is an EAP method based on symmetric cryptography and asymmetric key cryptography that reuses the TLS mechanisms. EAP-FAST has some nice features:

- ¸ TLV design that allows for extensibility
- ¸ Minimization of the per user authentication state requirement
- ¸ Handling of legacy equipment (use of TLS and MSCHAPv2)
- Fragmentation support

- ¸ Crypto-binding to allow sequence of EAP methods

However, this protocol has in my opinion two main drawbacks:

- Cryptographic design: choices were made to reuse flawed protocols (e.g. MSCHAPv2), new cryptographic designs were introduced without any explanations and the enrollment procedure is easily prone to attacks (especially in the anonymous Diffie-Hellman setting), which is acknowledged and justified by simplicity arguments. The cryptographic design could have benefited from the more evolved and secure password authentication techniques (e.g. EAP-SRP and EAP-SPEKE).
- It is quite a heavy weight protocol since for instance it refers to no less than 5 or 6 cryptographic primitives, namely a stream cipher - RC4, a block cipher - AES and hash functions - MD4, MD5 and SHA-1, and focuses directly on tunneling.

Regarding IPR, some IPR claims seem to be related to EAP-FAST, please refer to:

- http://www.ietf.org/ietf/IPR/cisco-ipr-draft-cam-winget-eap-fast.txt

EAP-FAST is an EAP method that has been allocated EAP Type 43 by IANA.

This method has been released very recently and should be further developed and implemented.

2.11 EAP-Archie

It is an EAP method proposed by Jesse Walker (Intel) and Russ Housley (Vigil Security).

The first version of it was proposed in February 2003 as an individual Internet-Draft: draft-jwalker-eap-archie-00.txt.

Version 01 published June 2003 is still to be found on the Internet.

It is an EAP method based on symmetric cryptography. It is very closely related to EAP-PSK since it was the main source of inspiration for EAP-PSK.

The main differences between EAP-Archie and EAP-PSK are:

- Some cryptographic changes (use of OMAC in EAP-PSK instead of CBC-MAC that cannot handle variable length messages, use of a key derivation scheme that has been proven to be secure in EAP-PSK, use of EAX to set up a protected channel, removal of the AES key wrap algorithm from EAP-PSK)

- o Some design changes (e.g. use of a TLV format in EAP-PSK instead of message types)

EAP-Archie will not be maintained and developed in the future ([EAP-Archie]), so EAP-PSK may be considered its successor in my opinion. Some implementations of EAP-Archie have been available.

2.12 EAP-GSS

GSS stands for Generic Security Service and is defined in RFC 2743.

It is an EAP method proposed by B. Aboba and D. Simon (Microsoft).

The first version of it was proposed in December 1999 under the title "PPP EAP GSS Authentication Protocol" as an individual Internet-Draft: draft-aboba-pppext-eapgss-00.txt.

Version 02 published November 2000, version 03 published February 2001, version 05 published July 2001, version 06 published August 2001, version 07 published August 2001, version 08 published September 2001, version 09 published December 2001, version 10 published January 2002, version 11 published February 2002 and version 12 published April 2002 are still to be found on the Internet. Hints to a version 01 and 13 may be found on the Internet but I did not manage to find the corresponding draft.

EAP-GSS enables the use of GSS-API mechanisms within EAP. As a result, any GSS-API mechanism providing initial authentication can be used with EAP GSS. Since some GSS-API mechanisms are shared key mechanisms, further investigation is required on this method (since I am currently not familiar with the GSS-API and GSS-API mechanisms).

2.13 EAP-IKEv2

IKEv2 stands for Internet Key Exchangev2.

It is an EAP method proposed by H. Tschofenig and D. Kroeselberg (Siemens) and Y. Ohba (Toshiba).

The first version of it was proposed in April 2003 as an individual Internet-Draft: draft-tschofenig-eap-ikev2-00.txt.

Version 01 published June 2003, version 02 published October 2003 and version 03 published August 2004 are still to be found on the Internet.

It is an EAP method based on the symmetric and asymmetric cryptography of IKEv2.

Its main advantages consist in my opinion consist first in reusing a protocol which security has received considerable expert review, second reusing a protocol that could become widely implemented and third benefiting from all the nice features provided by IKEv2 (mutual authentication, key derivation, DoS resistance, fast reconnect, fragmentation support,...). Further investigation is needed to assess this proposal that would be more generic than a shared key method replacing EAP-MD5 since it also allows for asymmetric credentials such as certificates(in particular studying the goals and different features of IKEv2 might be quite inspiring for EAP methods).

2.14 EAP-LDAP

LDAP is an EAP method proposed by H. Mancini (Bridgewater Systems).

The first version of it was proposed in June 2003 under the title "EAP-LDAP Protocol" as an individual Internet-Draft: draft-mancini-pppext-eap-ldap-00.txt.

Hints to a version 01 may be found on the Internet but I did not manage to find the corresponding draft.

This document specifies an EAP method to enable the use of EAP-MD5 even though there is no access to the user's clear text password within an identity store. It merely uses the hash of the user's password, hash which is stored within the identity store, as the key to EAP-MD5. It thus inherits at least all the vulnerability of EAP-MD5 and therefore is not suitable as a replacement for EAP-MD5.

2.15 EAP-MD5 Tunneled Authentication Protocol

EAP-MD5 Tunneled Authentication Protocol is an EAP method proposed by Paul Funk (Funk Software).

The first version of it was proposed in March 2003 under the title " The EAP MD5-Tunneled Authentication Protocol " as an individual Internet-Draft: draft-funk-eap-md5-tunneled-00.txt.

EAP-MD5-Tunneled is an EAP protocol designed for use as an inner authentication protocol within a tunneling EAP protocol such as EAP-TTLS or PEAP. It is cryptographically equivalent to standard CHAP and the EAP-MD5-Challenge protocol. Thus, EAP-MD5-Tunneled does not aim at proposing a generic shared key EAP method but rather the issues implied by tunneling EAP methods. In addition, EAP-MD5-Tunneled bears at least the same cryptographic weaknesses as EAP-MD5 and therefore is not suitable as a replacement for EAP-MD5.

2.16 EAP-PSK

EAP-PSK stands for EAP-Pre Shared Key.

It is an EAP method proposed by F. Bersani (France Telecom R&D).

The first version of it was proposed in January 2004 as an individual Internet-Draft: draft-bersani-eap-psk-00.txt.

Version 01 published February 2004 is still to be found on the Internet.

It is an EAP method based on symmetric cryptography. Its main design goals are:

- o Simplicity: It should be easy to implement and to deploy without any pre-existing infrastructure
- o Wide applicability: It should be possible to use this method to authenticate over any network. In particular, it should be suitable for IEEE 802.11 [IEEE 802.11] wireless LANs and thus comply to IEEE 802 EAP Method Requirements for Wireless LANs [IEEE 802REQ]
- o Security: It should be conservative in its cryptographic design and enjoy security proofs
- o Extensibility: It should be possible to add to this method the required extensions as their need appears
- o Patent-avoidance: It should be free of any Intellectual Property Right claims

It views itself as the successor of EAP-Archie.

It is intended to stimulate the debate on EAP-MD5 replacement and to be a proposal for such a replacement.

2.17 EAP-SKE

EAP-SKE stands for EAP Shared Key Exchange.

It is an EAP method proposed by L. Salgarelli (Bell Labs, Lucent Technologies) as the editor and many other co-authors.

The first version of it was proposed in November 2001 as an individual Internet-Draft: draft-salgarelli-pppext-eap-ske-00.txt.

Version 01 published April 2002, version 02 published November 2002 and version 03 published May 2003 are still to be found on the Internet. Hints to a version 04 may be found on the Internet but I did not manage to find the corresponding draft.

It is an EAP method based on symmetric cryptography. Its main focus is, in my opinion, network efficiency in roaming situations.

Work is going on between the authors of EAP-SKE and EAP-PSK to see if forces could be joined to produce a common proposal for a shared key method to the community [EAP-SKE].

2.18 EAP-SSC

SSC stands for Secured Smartcard Channel

It is an EAP method proposed by P.Urien and M. Dandjinou (ENST).

The first version of it was proposed in December 2003 under the title "EAP-SSC Secured Smartcard Channel " as an individual Internet-Draft: draft-urien-eap-ssc-00.txt.

Version 01 published June 2004 is still to be found on the Internet.

This document describes a means of setting up an EAP secured channel between a smart card and an Authentication Server as well according to an asymmetric key exchange model as a symmetric key exchange model. This channel would permit to convey securely all other types of payload between the smart card and the authentication server.

It is not clear what exactly makes the content of this document specific to a smart card. It seems to me as though the proposed protocol could be viewed as a generic symmetric and asymmetric cryptography EAP method. If so, the proposed cryptographic mechanism would require, in my opinion, expert review and justification to back up their soundness since new mechanisms seem to be introduced without justification. In addition, further investigation would be needed to assess the pros and cons of this protocol.

3. Conclusion

3.1 The different existing shared key EAP methods

This section attempts to provide a summary of the pros and cons of the existing shared key EAP methods listed in section 2.

EAP-MD5 has several security flaws that cannot be tolerated in the new environments where EAP is intended to be used like WLANs (e.g. no mutual authentication, no key derivation and high vulnerability to active brute-force/dictionary attacks). However, it has some nice features that might be worth keeping in mind: it is standardized and it is simple.

EAP-Cisco Wireless also has security flaws that should not be tolerated in the new environments where EAP is intended to be used like WLANs and it is an undocumented proprietary method. However, it

should be remembered as a proof of the need for a shared key EAP method as well as the feasibility of such a method.

MS-EAP-Authentication and EAP MSCHAPv2 unfortunately inherit, like EAP-Cisco Wireless, the intolerable security flaws of the protocol they are based on, namely MS-CHAPv2. A nice feature though to retain from these methods is the password aging and changing process.

EAP-MD5 Tunneled Authentication Protocol also inherit the weaknesses of EAP-MD5 and therefore cannot compete for its replacement.

EAP-SIM and EAP-AKA are not, in their design intention, generic shared key EAP methods. However in case, one wants to use them as such, EAP-SIM should be dropped in favor of EAP-AKA which is more evolved. Whether EAP-AKA could or should be reused as a generic shared key EAP method will be further investigated in the following versions of this draft, although the current feeling is that it should not.

EAP-HTTP Digest is a method designed to cope with legacy devices and protocols that is not publicly specified. It should therefore not impact the drafting of a replacement for EAP-MD5.

EAP-SRP and EAP-SPEKE are two very interesting methods for the drafting of a replacement for EAP-MD5 that use evolved cryptography to very efficiently deal with passwords. Further investigation is needed to assess whether or not such efficiency with passwords is required from a security point of view and whether it is possible to move forward with such techniques while avoiding IPR claims.

EAP-FAST is also an interesting method to take into account. However some choices it made seem to have been driven by a will to deal with legacy devices and infrastructures (e.g. reusing MS-CHAPv2). Further investigation is needed to determine whether dealing with legacy equipment should be a goal in the drafting of a replacement for EAP-MD5. EAP-FAST also provide fragmentation support. This leads to raising the question whether fragmentation support should be supported by the replacement of EAP-MD5 (the answer might be yes in my opinion since fragmentation support can probably be easily added and leaves the method open for future extensions that could require payloads larger than the MTU).

EAP-IKEv2 definitely requires further investigation to better understand IKEv2 design goals and features and whether they suit EAP well.

EAP-LDAP alludes to the possible problems that might arise when using a standard existing database to store the users' credentials. Similarly to EAP-FAST, further investigation is needed to see if

dealing with legacy devices and infrastructures should be a design goal and if yes, how to deal with them.

EAP SSC needs further investigation to better understand its goals and its capabilities as well as the security level it provides.

EAP GSS needs further investigation to assess to what extent it could be used in conjunction with a GSS-API mechanism to be specified to replace EAP MD5. The nice idea behind EAP GSS is the use of a generic API to access a range of different authentication mechanisms, although this might be redundant with EAP itself.

Hopefully, EAP-PSK (which may be considered EAP-Archie's successor since EAP-Archie will not be further developed) and EAP-SKE will be merging to propose a base draft to the community for replacing EAP-MD5. It is believed to have a sound security basis as well as a simple and extensible design.

3.2 General conclusion on shared key EAP methods

There is a wide range of existing shared key EAP methods which is good since it demonstrates the creativity of the community but is also dangerous since it first dilutes the review effort of the community which might result in flawed or broken protocols and second it does not help to provide interoperability.

Thanks to all the good ideas contained in the drafts mentioned in the precedent section, it seems to be quite possible to draft a standard replacement for EAP-MD5 that would retain the best of all worlds, provided the community shows interest in doing so.

Further work is needed to better assess the status of the different drafts mentioned in the precedent section and understand their pros and cons (especially those of EAP-AKA, EAP-FAST, SRP-SHA1, EAP-SPEKE, EAP GSS, EAP-PSK and EAP SSC). Hopefully, this will be done in future versions of this document.

Most drafts do not comply to EAPbis or EKMF which understandable since those documents were themselves evolving.

It would be a good idea to clarify the relationship between shared key EAP methods and OTP methods (since they both tend to use the same symmetric cryptography credentials). Hopefully, this will be done in future versions of this document.

3.3 Miscellaneous conclusions

Similar unification work could be done in the following areas:

- o OTP EAP methods (in case, they are deemed essentially different from EAP methods as a result of the further investigations announced in the previous subsection)
- o Biometrics EAP method (since like OTP EAP methods, there are numerous candidates available, yet none has acquired the maturity and extent of a widespread standard)
- o Public key EAP methods (although EAP-TLS has already emerged as a standard)
- o Hybrid methods (i.e. using public key on one side and private key on the other side)

Such work could improve the quality of the methods and help users find they way through the myriads of EAP methods!

4. Review of the non shared key EAP methods

The EAP methods presented here have been included for the sake of completeness: they are deemed totally irrelevant for the drafting of a replacement for EAP-MD5.

4.1 EAP-OTP

EAP-OTP stands for one-time password.

Please refer to [EAP] and [EAPbis] for a description of EAP-OTP, which is thus a standardized method.

This EAP method has been defined for use with one-time password systems.

Unfortunately, this method is quite simplistic and outdated (see for instance the security claims in [EAPbis]). Therefore, this method is, in my opinion, only specified for legacy reasons and its security and functionality levels do not match the current requirements.

4.2 EAP-GTC

EAP-GTC stands for generic token card.

Please refer to [EAP] and [EAPbis] for a description of EAP-GTC, which is thus a standardized method.

This EAP method has been defined for use with various token card implementations that require user input. It consists in a challenge (containing a displayable message) and a response (containing the data entered by the user from the token card).

Unfortunately, this method is so simplistic and outdated (since in only a round-trip, it is quite hard to provide a good level of

security - see for instance the security claims in [EAPbis]) that many token cards have chosen to develop their own methods (see e.g. section 4.8). Therefore, this method is, in my opinion, only specified for legacy reasons and its security and functionality levels do not match the current requirements.

4.3 EAP RSA Public Key Authentication

EAP-RSA PKA stands for EAP RSA Public Key Authentication Protocol.

It is an EAP method proposed by William T. Whelan (Network Express and later Cabletron Systems).

The first version of it was proposed in November 1995 as a PPPEXT WG Internet-Draft: draft-ietf-pppext-eaprsa-00.txt.

Version 01 published February 1996, version 02 published February 1996, Version 03 published January 1997 and Version 03 published January 1997 are still to be found on the Internet.

EAP-RSA PKA is an EAP method that has been allocated EAP Type 9 by IANA.

It is an EAP method based on asymmetric cryptography and the unilateral two pass authentication described in ISO/IEC 9798-3.

It seems to be subject to patents by RSA Security, see http://www.ietf.org/ietf/IPR/pppext-eaprsa

This method does not seem to be maintained any more.

4.4 EAP-DSS

EAP-DSS stands for EAP DSS Public Key Authentication Protocol and DSS stands for Digital Signature Standard.

It is an EAP method proposed by William A. Nace (NSA) and James E. Zmuda(SPYRUS).

The first version of it was proposed in November 1997 as a PPPEXT WG Internet-Draft: draft-ietf-pppext-eapdss-00.txt.

Version 01 published December 1997 is still to be found on the Internet. Hints to a version 02 may be found on the Internet but I did not manage to find the corresponding draft.

EAP-DSS is an EAP method that has been allocated EAP Type 10 (Under the name DSS Unilateral) by IANA.

It is an EAP method that uses asymmetric cryptography (namely the DSA) and is based on unilateral two pass authentication as described in NIST FIPS PUB 196 "Standard for Public Key Cryptographic Entity Authentication Mechanisms".

This method does not seem to be maintained any more.

4.5 EAP-KEA

EAP-KEA stands for EAP KEA Public Key Authentication Protocol and KEA stands for Key Exchange Algorithm.

It is an EAP method proposed by William A. Nace (NSA), Peter Yee and James E. Zmuda (both of SPYRUS).

The first version of it was proposed in November 1997 as a PPPEXT WG Internet-Draft: draft-ietf-pppext-eapkea-00.txt.

Version 01 published December 1997 is still to be found on the Internet. Hints to a version 02 may be found on the Internet but I did not manage to find the corresponding draft.

EAP-KEA is an EAP method that has been allocated EAP Types 11 and 12 by IANA.

It is an EAP method that uses asymmetric cryptography (namely Diffie-Hellman).

This method does not seem to be maintained any more.

4.6 EAP-TLS

Please refer to [EAP-TLS] for a description of this method.

EAP-TLS is an EAP method that has been allocated EAP Type 13 (by IANA.

EAP-TLS is an EAP method based on asymmetric cryptography reusing TLS mechanisms.

4.7 Defender Token (AXENT)

Defender Token (AXENT) is an EAP method that has been registered to IANA by Michael Rosselli (Axent).

It is an undocumented EAP method. The contact information indicated in IANA is outdated (AXENT has been merged to Symantec then sold to Passgo). Information request has been requested to Passgo which kindly provided some ([Defender]).

Defender Token (AXENT) is an EAP method that has been allocated EAP Type 34 by IANA.

The Defender Token (AXENT) EAP method was never completed. PassGo Technologies may continue this development at some point in the future but there are no immediate plans to do so at present.

4.8 RSA Security SecurID EAP and SecurID EAP

Two EAP types have been allocated by IANA for RSA SecurID authentication: type 15 and type 32.

Some documentation on these methods have been kindly communicated by [RSA SecurID].

EAP type 15 was developed for use with RSA Security clients and Agents on the Windows platform. It is proprietary and may remain that way.

Seeing the need for an open EAP type to support RSA Tokens, EAP type 32 has been reserved.

It is an EAP method proposed by S. Josefsson (RSA Security).

The first version of it was proposed in January 2002 as an individual Internet-Draft: draft-josefsson-eap-securid-00.txt.

Version 01 published February 2002 is still to be found on the Internet. Hints to a version 02 may be found on the Internet but I did not manage to find the corresponding draft.

Temporarily there does not seem to be any (public) work done is this method any more.

Both methods are basically OTP methods that rely on the RSA SecurID authentication token.

4.9 Arcot systems EAP

Arcot systems EAP is an EAP method that has been registered to IANA by Rob Jerdonek (Arcot).

It is an undocumented EAP method. Information has been requested from Arcot but no answer has yet been obtained.

Arcot systems EAP is an EAP method that has been allocated EAP Type 16 by IANA.

Arcot systems EAP is an EAP method that probably relies on a OTP scheme using a software authentication token. It should therefore not compete as a replacement for EAP-MD5 (see [Arcot] for general information).

4.10 EAP-TTLS

EAP-TTLS stands for EAP Tunneled TLS Authentication Protocol.

It is an EAP method proposed by Paul Funk (Funk Software) and Simon Blake-Wilson (Certicom).

The first version of it was proposed in August 2001 as a PPEXT WG Internet-Draft: draft-ietf-pppext-eap-ttls-00.txt.

Version 01 published February 2002, version 02 published November 2002, version 03 published August 2003 are still to be found on the Internet. Hints to a version 04 may be found on the Internet but I did not manage to find the corresponding draft.

EAP-TTLS is an EAP method that has been allocated EAP Type 21 by IANA.

EAP-TTLS is an EAP method based on asymmetric cryptography reusing TLS mechanisms. In EAP-TTLS, the TLS handshake may be mutual; or it may be one-way, in which only the server is authenticated to the client. The secure connection established by the handshake may then be used to allow the server to authenticate the client using existing, widely-deployed authentication infrastructures such as RADIUS. The authentication of the client may itself be EAP, or it may be another authentication protocol such as PAP, CHAP, MS-CHAP or MS-CHAP-V2.

4.11 Remote Access Service

Remote Access Service is an EAP method that has been registered to IANA by Steven Fields (Identix).

It is an undocumented EAP method. Information has been requested from Identix but no answer has yet been obtained.

Remote Access Service is an EAP method that has been allocated EAP Type 22 by IANA.

It is not clear to me how this EAP method works (though it probably relies on biometrics, see [Identix] for general information).

4.12 EAP-3Com Wireless

EAP-3Com Wireless is an EAP method that has been registered to IANA by Albert Young (3com).

It is an undocumented EAP method. Information has been requested from but no answer has yet been obtained (the contact information indicated in IANA is outdated).

EAP-3Com Wireless is an EAP method that has been allocated EAP Type 24 by IANA.

It is not clear to me how this EAP method works (See [3com] for general information).

4.13 PEAP

PEAP stands for Protected Extensible Authentication Protocol.

It is an EAP method proposed by H. Andersson (RSA Security), S. Josefsson (RSA Security and later Extundo), Glen Zorn and Hao Zhou (Cisco), Dan Simon and Ashwin Palekar (Microsoft).

The first version of it was proposed in August 2001 as an individual Internet-Draft under the title "Protecting EAP with TLS (EAP-TLS-EAP)": draft-josefsson-pppext-eap-tls-eap-00.txt.

Version 01 published October 2001, version 02 published February 2002, version 03 published September 2002, version 04 published September 2002, version 05 published September 2002, version 06 published March 2003, version 07 published October 2003 are still to be found on the Internet.

PEAP is an EAP method based on asymmetric cryptography reusing TLS mechanisms that has been allocated EAP Type 25 by IANA.

PEAP is an EAP method based on asymmetric cryptography reusing TLS mechanisms which provides an encrypted and authenticated tunnel based on transport layer security (TLS) that encapsulates EAP authentication mechanisms. PEAP uses TLS to protect against rogue authenticators, protect against various attacks on the confidentiality and integrity of the inner EAP method exchange and provide EAP peer identity privacy. EAP also provides support for chaining multiple EAP mechanisms, cryptographic binding between authentications performed by inner EAP mechanisms and the tunnel, exchange of arbitrary parameters (TLVs), optimized session resumption, and fragmentation and reassembly.

Regarding IPR, some IPR claims seem to be related to EAP-FAST, please refer to: http://www.ietf.org/ietf/IPR/MICROSOFT-PEAP.txt

4.14 EAP-MAKE

EAP-MAKE stands for EAP Mutual Authentication with Key Exchange.

It is an EAP method proposed by R. Berrendonner and H. Chabanne (both of Sagem).

The first version of it was proposed in September 2001 as an individual Internet-Draft: draft-berrendo-chabanne-pppext-eapmake-00.txt.

Version 01 published October 2001 is still to be found on the Internet. Hints to a version 02 may be found on the Internet but I did not manage to find the corresponding draft.

EAP-MAKE is an EAP method that has been allocated EAP Type 27 by IANA.

It is an EAP method inspired by EAP-KEA that uses asymmetric cryptography (namely Diffie-Hellman).

This method does not seem to be maintained any more.

4.15 CRYPTOcard

CRYPTOcard is an EAP method that has been registered to IANA by Stephen Webb (Cryptocard).

It is an undocumented EAP method. Information has been requested from CRYPTOcard but no answer has yet been obtained (there seemed to be a problem with the mail box of the contact indicated by IANA and no answer was yet obtained from the general support).

CRYPTOcard is an EAP method that has been allocated EAP Type 28 by IANA.

It is not clear to me how this EAP method works (it is probably an EAP method that relies on an authentication token, see [CRYPTOcard] for general documentation).

4.16 DynamID

DynamID is an EAP method that has been registered to IANA by P. Merlin (SCrypto).

It is an undocumented EAP method, though some elements were kindly provided by [DynamID]..

DynamID is an EAP method that has been allocated EAP Type 30 by IANA.

It is an EAP method that uses asymmetric key cryptography (namely digital certificates stored on smart cards). It is a challenge-response method that only provides client authentication. This method also provides key derivation.

4.17 Rob EAP

Rob EAP is an EAP method that has been registered to IANA by Sana Ullah.

It is an undocumented EAP method. Information has been requested from Sana Ullah but no answer has yet been obtained.

Rob EAP is an EAP method that has been allocated EAP Type 31 by IANA.

It is not clear to me how this EAP method works (I found absolutely no information on it!).

4.18 MS-Authentication TLV

TLV stands for Type-Length-Value.

It is an EAP method proposed by T. Hiller (Lucent), A. Palekar (Microsoft) and G. Zorn (Cisco).

The first version of it was proposed in October 2002 under the title "A Container Type for the Extensible Authentication Protocol (EAP)" as an individual Internet-Draft: draft-hiller-eap-tlv-00.txt.

Version 01 published May 2003 is still to be found on the Internet. Hints to a version 02 may be found on the Internet but I did not manage to find the corresponding draft.

MS-Authentication TLV is an EAP method that has been allocated EAP Type 33 (Under the name DSS Unilateral) by IANA.

It is not really an authentication method but a proposed solution to some issues that arose within the EAP WG.

4.19 SentriNET

SentriNET is an EAP method that has been registered to IANA by J. Kelleher (ISL Biometrics).

It is an undocumented EAP method, though some elements were kindly provided by [SentriNET].

SentriNET is an EAP method that has been allocated EAP Type 34 by IANA.

SentriNET (per se, not the EAP method that bears the same name) is a biometric middleware product which adds biometrics to existing user accounts in their native location (e.g. NT SAM accounts, Active Directory, LDAP entries or entries in a database for web applications). Management and checking of these biometrics is similarly integrated (e.g. MMC and GINA for Microsoft Windows 2000/XP, ...).

SentriNET (the EAP method) is a method designed to extend the biometric logon available to local users to remote access via a NAS or VPN.

SentriNET (the EAP method) remains proprietary with no plans for publication in the near future. Its basic operation involves the supplying of a user name to the server which checks which biometrics have been enrolled and returns information on the appropriate hardware types to the client, the client captures a live biometric on a suitable device and returns it to the server for matching.

4.20 EAP-Actiontec Wireless

EAP-Actiontec Wireless is an EAP method that has been registered to IANA by Victor Chang (Actiontec)

It is an undocumented EAP method. Information has been requested from Actiontec but no answer has yet been obtained.

EAP-Actiontec Wireless is an EAP method that has been allocated EAP Type 35 by IANA.

It is not clear to me how this EAP method works (see [Actiontec] for general documentation).

4.21 Cogent systems biometrics authentication EAP

Cogent systems biometrics authentication EAP is an EAP method that has been registered to IANA by John Xiong (Cogent systems)

It is an undocumented EAP method. Information has been requested from Cogent systems but no answer has yet been obtained.

Cogent systems biometrics authentication EAP is an EAP method that has been allocated EAP Type 36 by IANA.

It is not clear to me how this EAP method works though it probably relies on biometrics (see [Cogent] for general documentation).

4.22 AirFortress EAP

AirFortress EAP is an EAP method that has been registered to IANA by Richard Hibbard (Fortress technologies)

It is an undocumented EAP method. Information has been requested from Fortress technologies but no answer has yet been obtained.

AirFortress EAP is an EAP method that has been allocated EAP Type 37 by IANA.

It is not clear to me how this EAP method works (see [Airfortress] for general documentation).

4.23 Securesuite EAP

Securesuite EAP is an EAP method that has been registered to IANA by Matt Clements (Iosoftware).

It is an undocumented EAP method. Information has been requested from Iosoftware but no answer has yet been obtained.

Securesuite EAP is an EAP method that has been allocated EAP Type 39 by IANA.

It is not clear to me how this EAP method works (see [Securesuite] for general documentation).

4.24 DeviceConnect EAP

DeviceConnect EAP is an EAP method that has been registered to IANA by David Pitard (Phoenix).

It is an undocumented EAP method. Information has been requested from Phoenix but no answer has yet been obtained.

DeviceConnect EAP is an EAP method that has been allocated EAP Type 40 by IANA.

It is not clear to me how this EAP method works (see [DeviceConnect] for general documentation).

4.25 EAP-MOBAC

EAP-MOBAC is an EAP method that has been registered to IANA by T. Rixom (Alfa-Ariss).

It is an undocumented EAP method, though some elements were kindly provided by [EAP-MOBAC].

EAP-MOBAC is an EAP method that has been allocated EAP Type 42 by IANA.

It is an EAP method that is basically OTP via SMS. It thus requires a special infrastructure (gateway to the SMS system and OTP server) and is therefore not a possible candidate for EAP-MD5 replacement.

4.26 ZoneLabs EAP (ZLXEAP)

ZoneLabs EAP is an EAP method that has been registered to IANA by D. Bogue (ZoneLabs).

It is an undocumented EAP method, though some elements were kindly provided by [ZoneLabs].

ZoneLabs EAP is an EAP method that has been allocated EAP Type 44 by IANA.

It is an EAP method that should augment shared key EAP methods, not replace them.

4.27 EAP Bluetooth Application

EAP Bluetooth Application is an EAP method proposed by H. Kim (INRIA), H. Afifi (INT) and M. Hayashi (Hitachi).

The first version of it was proposed in February 2004 as an individual Internet-Draft under the title "EAP Bluetooth Application": draft-kim-eap-bluetooth-00.

EAP Bluetooth Application is not an authentication method but rather a way to help to Bluetooth devices set up a secure channel thanks to EAP authentication through a IEEE 802.11 interface of one of the devices. It therefore merely tunnels other EAP authentication methods for what regards authentication.

4.28 EAP-GPRS

GPRS stands for General Packet Radio Service (it is a concept imported from the GSM world).

It is an EAP method proposed by A. Salkintzis (Motorola).

The first version of it was proposed in December 2002 under the title "The EAP GPRS Protocol" as an individual Internet-Draft: draft-salki-pppext-eap-gprs-00.txt.

Version 01 published June 2003 and version 02 published January 2004 are still to be found on the Internet.

EAP-GPRS specifies an extension to EAP which allows GPRS clients to perform signaling procedures with a core GPRS network through devices that enforce EAP-based access control. For example, a GPRS client can use EAP-GPRS to attach to a GPRS network through an access point that enforces IEEE 802.1X access control. In this case, the GPRS attach signaling is performed in the context of the underlying 802.1X procedure and the GPRS messages are encapsulated into EAP-GPRS packets. If the GPRS client is permitted to attach to the GPRS network, then the 802.1X procedure ends successfully and the client is authorized access to the access point. In general, EAP-GPRS allows any type of signaling to take place during the EAP authentication as an embedded signaling procedure.

It is not really an authentication method but rather a new transport mechanism for higher-layer protocols.

4.29 EAP support in smart cards

EAP support in smart cards is an EAP method proposed by P. Urien (ENST), A. J. Farrugia (CSI), G. Pujolle (LIP6), J. Abellan (Axalto) and M. de Groot (Gemplus).

The first version of it was proposed in October 2002 as an individual Internet-Draft under the title "EAP support in smartcards ": draft-urien-eap-smartcard-00.txt.

Version 01 published February 2003, version 02 published June 2003, version 03 published September 2003 and version 04 published February 2004 are still to be found on the Internet.

EAP support in smart cards is not an authentication method but rather describes the interface to the EAP protocol in smart cards, which could store multiple identities associated to Network Access Identifiers. It therefore merely tunnels other EAP authentication methods for what regards authentication.

4.30 EAP-TLS SASL

SASL stands for Simple Authentication and Security Layer.

It is an EAP method proposed by H. Andersson and S. Josefsson (RSA Security).

The first version of it was proposed in June 2001 under the title "EAP Mechanism using TLS and SASL (Version 1)" as an individual Internet-Draft: draft-andersson-eap-tls-sasl-00.txt.

Hints to a version 01 may be found on the Internet but I did not manage to find the corresponding draft.

The development of this method seem to have been stopped as its authors moved to work on PEAP (please refer to section 4.13).

5. IANA considerations

This document does not introduce any new IANA consideration.

6. Security considerations

This document does not introduce any new security issue for the Internet.

7. Acknowledgements

Many thanks to the EAP WG chairs (J. Arkko and B. Aboba) for motivating this work, to Laurent Butti, Olivier Charles, Aurelien Magniez and Jerome Razniewski for their feedback and to all those mentioned in the References section that kindly took some time to answer some of my questions!

Special thanks to Henri Gilbert for some related cryptographic discussions on shared key EAP methods.

8. References

[Actiontec]   http://www.actiontec.com

[AirFortress]   http://www.fortresstech.com/

[Arcot]   http://www.arcot.com/

[CHAP]   Simpson, W., "PPP Challenge Handshake Authentication
                Protocol (CHAP)", RFC 1994, August 1996.

[Cogent]   http://www.cogentsystems.com/cogent/cogenthome.html

[CRYPTOcard]   http://www.cryptocard.com/

[Defender]   Peter Cooke, PCooke@passgo.com,
                Personal communication, March 2004

[DeviceConnect] http://www.phoenix.com/en/products
                /phoenix+deviceconnect/default1.htm

[Dynamid]   P Merlin (Scrypto), pmerlin@scrypto.fr,

Personal Communication, March 2004

[EAP] Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[EAP-Archie] Russ Housley and Jesse Walker, Personal communications, February 2004

[EAPbis] Blunk, L. et al., "Extensible Authentication Protocol (EAP)", Internet-Draft (work in progress), February 2004, http://ietf.levkowetz.com/drafts/eap/rfc2284bis/draft-ietf-eap-rfc2284bis-09.txt

[EAPHTTPDigest] O. Tavakoli (Funk Software), radagast@funk.com, Personal Communication, March 2004

[EAPIssues] EAP Open issues list, http://www.drizzle.com/~aboba/EAP/eapissues.html

[EAP-METHSTAT1] Aboba B., "EAP and AAA update", NIST 802.11 security workshop, December 2002, http://csrc.nist.gov/wireless/S12_NIST-IETFpart2--ba.pdf

[EAP-METHSTAT1] Arkko J. and Aboba, B., "EAP WG Methods Update", IETF 59, March 2004, http://www.arkko.com/publications/eap/ietf-59/ietf59_eap_methstatus.ppt

[EAP-MOBAC] T. Rixom (Alfa-Ariss), tom.rixom@alfa-ariss.com, Personal Communication, March 2004

[EAP-PSK] Bersani, F., "The EAP-PSK protocol", Internet-Draft (work in progress), February 2004, draft-bersani-eap-psk-01.txt

[EAP-SKE] Luca Salgarelli, Uri Blumenthal and Semyon Mizikovski, Personal communications, February and March 2004

[EAP-SKMDTEMPL] Bersani, F., " EAP shared key methods documentation template", Internet-Draft (work in progress), March 2004, draft-bersani-eap-sharedkeymethods-doctemplate-00.txt

[EAP-TLS] Aboba, B., Simon, D., "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[EKMF] Aboba, B. et al., "EAP Key Management Framework",

Internet-Draft (work in progress), October 2003, draft-ietf-eap-keying-01.txt

[HTTP-Digest] Franks, J. et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999

[IANA] Internet Assigned Numbers Authority, "Point-to-Point Protocol Field Assignments/PPP EAP Request/Response Types", http://www.iana.org/assignments/ppp-numbers

[Identix] http://www.identix.com/

[IEEE 802.1X] IEEE STD 802.1X, Standards for Local and Metropolitan Area Networks: Port Based Access Control, June 14, 2001

[IEEE 802.11] Institute of Electrical and Electronics Engineers, "Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements û Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard 802.11

[IEEE 802REQ] Stanley, Dorothy et al., ôEAP Method Requirements for Wireless LANsö, Internet-Draft (work in progress), January 2004, draft-walker-ieee802-req-00.txt

[LEAP] Macnally, C., ôCisco LEAP protocol descriptionö, September 2001

[LEAPVUL] Wright, J., ôWeaknesses in LEAP Challenge/Responseö, Defcon 2003

[MDx] Preneel, B. and van Oorschot P. C., "MDx-MAC and Building Fast MACs from Hash Functions", Proceedings of Crypto'95, Springer-Verlag, LNCS, August 1995

[MSCHAPVUL] Schneier, B. and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", CQRE '99, Springer-Verlag, 1999, http://www.schneier.com/paper-pptpv2.pdf

[PPP] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RSA SecurID] D. Liberman (RSA Security),

dliberman@rsasecurity.com, Personal Communication,
March 2004

[Securesuite] http://www.iosoftware.com/pages/Products/SecureSuite%20XS/index.asp

[SentriNET] J. Kelleher (ISL Biometrics),
joe.kelleher@isl-biometrics.com,
Personal Communication, March 2004

[SRP] The Stanford SRP Authentication Project,
http://srp.stanford.edu/

[SRPpres] Wu, T., "Secure Remote Password Authentication",
NDSS 98 , http://srp.stanford.edu/ndss98s.ps

[ZoneLabs] D. Bogue (ZoneLabs), dbogue@zonelabs.com,
Personal Communication, March 2004

[3com] http://www.3com.com

9. Authors' Addresses

Florent Bersani   florent.bersani@francetelecom.com
France Telecom R&D
38, rue du General Leclerc
92794 Issy Les Moulineaux Cedex 9
France

10. Full Copyright Statement