CONNOTECH Experts-conseils inc.

Pre-Shared Secret Authentication Challenges, a Survey and the SAKEM Proposal (the SAKEM[1] White Paper)

Document Number C003323

2005/03/01

Thierry Moreau
e-mail: thierry.moreau@connotech.com

Document Revision History

C-Number	Date	Explanation
C003323	2005/03/01	First release

[1] SAKEM: Secret Authentication Key Establishment Method. Other acronyms are listed on page 12.

Introduction

Introduction

This document attempts to survey the reliance on pre-shared secrets in various types of information security schemes. Modern information security makes use of cryptographic techniques, broadly segregated in symmetric key cryptography and public key cryptography. Our focus is on the very initial authentication of cryptographic keys, for which we attempt to show a commonality of requirements despite very diversified documentation approaches. In the second part of this document, we present the SAKEM proposal, a practical solution applicable to the symmetric case (page 7).

Documentation Approaches to Initial Confidence

Initial confidence on cryptographic keys

In many fielded information security schemes, a central database of cryptographic keys serves as the foundation for transaction authentication. The question we whish to address is the ultimate rationale behind the *initial* confidence, or trust, in the association between cryptographic keys and the entities represented by them. A representative case is on-line treasury management services offered by banks to large corporate and government entities (large value payment transactions initiated electronically and secured by some form of cryptographic authentication). On an on-going basis, the bank confidence in its key database rests on the absence of fraud incidents and the assumption that corporate and government comptroller offices do maintain internal controls minimizing the likelihood of key compromise. Turning to the initial confidence on a single cryptographic key, the rationale is either a recursive re-use of cryptographic mechanisms (e.g. a PKI), or reliance on some procedural means, out-of-band distribution, manual distribution, two-person-control distribution, secure courier, mandatory in-person validation.

A temptative survey methodology

The above example is representative of the *initial confidence on cryptographic keys* upon which rests most security schemes, and the relevance of *procedural steps*. However, the security scheme description documents relate to these issues with very diversified documentation strategies, ranging from the lack of any reference (i.e. assuming that the reader has a prior understanding), to specific procedural means to achieve the required initial authentication. We propose a survey methodology as a attempt to highlight the commonality of reliance on initial confidence on keys and procedural steps. The method applies a series of questions to information security scheme documents.

Question 1

Q.1 Is the document describing a *security scheme* that would provide a

security scheme

defined security service to an application, if the scheme is implemented?

Q.1 "no"

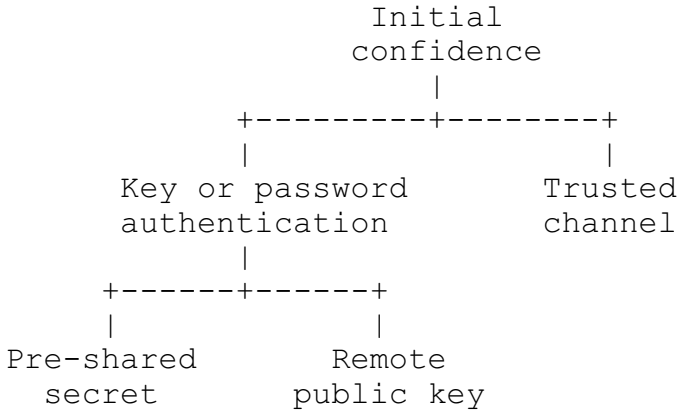
This question is intended to leave out the documents for which the deployment issues are too remote. For instance a cryptography primitive algorithm (block cipher, digital signature, ...) does not provide confidentiality or data origin authentication without provisions for mode of operation, message blocking, key management, protocol. Also, some quality standards are mainly auditor's tools and are not describing any particular scheme ([1], [2]).

Question 2 scheme deployment

Q.2 Is the security scheme deployment based on some *authenticated key or secret* or a *trusted channel*, e.g. out-of-band distribution, but other than a CA or root certification public key?

Initial confidence concepts

The following hierarchy of concepts is useful to identify where a scheme description refers to the initial confidence on which the scheme resides. The hierarchy shows (on its left side) the explicit references to cryptographic key authentication, refined into the symmetric case and the public key case. Assuming that a "trusted channel" exists as shown on the right in the hierarchy, any kind of initial confidence can be set up. Indeed, many scheme descriptions refer to a trusted channel as their single reference to the initial confidence issue. An explicit reference to initial confidence in a security scheme description will often recognize the need of procedural steps in the deployment phase. As a general note, when reading a security scheme description, one should be cautious about bird's eye view of the protocols, which do not occur in practice: each participant separately experiences its role, with its own set of threats, adversaries, and potential incidents. Trust and confidence issues should be understood accordingly.



Types of key or secret

At this stage, we should observe the type of key or secret to be authenticated or delivered through the trusted channel, among

a) a symmetric secret key,
b) a shared secret password,
c) trust in a remote party's public key, and
d) the delivery of a private key from a key generation service to its intended user entity.

Our survey methodology makes no distinction on the type of key or secret on the argument that one type can be converted into another using "well known" cryptographic mechanisms, at least among types a) to c). If a symmetric secret key exists, a password can be established with encryption under that key and a remote party's public key can be authenticated by the remote party's ability to apply its alleged private key to a value properly derived from the symmetric key. In the other direction, there are key management schemes that claim to turn passwords and low entropy secrets into secure cryptographic keys ([3]). Key transport and key agreement schemes ([4]) turn an authenticated remote party's public key into a symmetric key.

A unique level of initial confidence applies to the type d) above (delivery of a private key from a key generation service to an end-user), i.e. the end-user is expected to trust the service provider as a potential key escrow agent (public key schemes are otherwise documented as immune to impersonation threats) and a service provider is often also a CA which needs assurance about the end-user compliance to PKI guidelines before issuing a security certificate. Since our focus is on the commonality of initial assurance mechanisms, these demanding requirements are merely anecdotical. Security scheme provisions that meet them should meet the confidence expectations for other types or key or secrets. In the other direction, a pre-shared symmetric key can provide the required distribution channel if the symmetric key assurance are adequate.

Q.2 "no"

We arbitrarily set apart the PKI components that make routine use of a root public key (either a root CA or a "trust anchor" key). In practice, the distribution of a root public key is perhaps the most elementary procedural action for any cryptographic scheme deployment. An instance of an excluded scheme is the TLS protocol with an unauthenticated client ([5], [6]), which is bootstrapped by root public keys embedded in browser software. Note that this PKI routine component exception does not exclude the PKI client certificate issuance schemes, because these require the trust in a remote client's public key. Other fairly common key management

techniques might have been left outside our survey scope, e.g. the derivation of session keys from long-term keys with perfect forward secrecy.

Question 3 procedural steps

Q.3 Does the scheme document specify the *procedural steps* required to authenticate the key?

Q.3 "yes"

We suggest that a "yes" answer applies to a small number of previous work publications. Some examples:

- a scheme where hash values are to be compared out-of-band before a CA issues a security certificate to a PKI client ([7]),
- out-of-band publication for root key compromise recovery ([8]),
- a scheme for field initialization of network devices using time windows as authentication evidence ([9]), and
- the SAKEM scheme described in the second part of the present document.

Q.3 "no"

If answers to Q.1, Q.2, and Q.3 are "yes," "yes," and "no," the documented information security scheme deserves attention to the procedural aspects of deployment.

Question 4 implicit

Q.4 Is the key authentication or trusted channel requirement merely implicit or somehow out-of-scope?

Question 4.1 barrier to market entry

Q.4.1 If "yes," does the document define compliance in a context that makes the document a barrier to entry into a segment of the information security market?

Q.4 "yes"
Q.4.1 "yes"

Some security scheme descriptions are standards, with a notion of conformance for implementation certification. We found some cases where the initial key authentication issue is left out of compliance requirements (answer to Q.4 is "yes") and this omission lowers conformance requirements, facilitating entry into some information security markets (answer to Q.4.1 is "no"):

- A recent NIST initiative on electronic authentication, where no provisions address the link between "identity proofing" and "delivery of credentials" ([10]). Presumably, the short time frame for issuance of this standard, and then the availability of compliant products for US government procurement, prevented adoption of demanding provisions for authentication key delivery. We believe that NIST missed the opportunity to explicitly link the electronic authentication techniques to sensible key management guidelines, including the challenges of binding a pre-shared secret to an

identity.

- The PKI initiative development was tainted by policy and liability issues when a relevant Internet document, RFC2510, was first issued ([11], [12]). Perhaps the non-mandatory nature of the "initial authentication key" in RFC2510 was motivated by the need to facilitate the compliance of certification practice statements.
- In European quality standards for electronic signatures, the standardization committee left out of scope the trusted channel requirements for the delivery of a private key from a key generation service to an end-user ([13]).

Q.4 "yes"
Q.4.1 "no"

More commonly, the answer to Q.4 is "yes" without market forces influence, i.e. answer to Q.4.1 is "no". This category should contain a large number of documents with implicit references to the initial confidence on cryptographic keys, or a trusted channel needed to establish them. Arbitrarily selected examples include [14], [15], and [16].

Q4 "no"

A "no" answer to Q.4 applies to a number of documents saying that some out-of-band requirement exists, that the out-of-band technique must provide appropriate assurance about the remote party, and that these issues should be addressed for a secure implementation.

Question 5 at-par provisions

Q.5 Are there at-par provisions for pre-shared secret authentication *and* remote public key confidence?

Q.5 "yes"

A "yes" answer to Q.5 means a document where secure deployment can use either an authenticated secret key distribution, or a trust mechanism for remote public key, *referring to procedural means in either case*. When a security scheme design allows this flexibility between a symmetric and a public key solution, this documentation approach carries the flexibility to the implementation phase where out-of-band authentication means are to be provided. Here are some examples:

- a recent scheme proposal where a server (perhaps co-located with the CA function) supplies a private keys to PKI participants ([17]),
- a recent proposal in the field of Internet telephony ([18]), and
- the abovementioned PKI certificate issuance scheme ([7]).

Documents in which an implementation choice is provided between a recursive reuse of yet another cryptographic scheme and an out-of-band mechanism (e.g. either a pre-shared secret or a public key backed by a PKI certificate) should not be mistaken as a "yes" to Q.5.

Q.5 "no"

This category should contain a large number of documents with explicit

reference to key or password authentication. Arbitrarily selected examples include [19], [20], [21], [22], and [23].

Summary

The classification questionnaire creates two general documentation patterns with respect to the initial confidence on keying material used in a cryptographic scheme:

- the implicit references (Q.4.1 "no") and
- the explicit references (Q.5 "no"),

and three exception patterns,

- the specific procedural steps documentation (Q.3 "yes")
- the compliance facilitation for reduced market entry barriers (Q.4.1 "yes"), and
- the procedural steps implementation flexibility, i.e. reliance on either symmetric-key or public-key initial authentication (Q.5 "yes").

When the implicit reference documentation pattern is followed, the reader has to identify which keys or passwords are to be protected by a trusted channel. For this classification, we amalgamated the procedural requirements for pre-shared secrets (symmetric keys and passwords) and public keys.

The SAKEM Proposal

SAKEM (Secret Authentication Key Establishment Method)

The SAKEM proposal is an attempt to gracefully mate technology-intensive cryptographic mechanisms to the practicalities of procedural means. Its account is rigorous when addressing the cryptographic portion, and more descriptive when providing procedural guidance. The SAKEM proposal pertains to the business processes for secure application and secure network deployment. In designing such business processes, the tendency to automate any task has to yield to the authentication requirements for "out-of-band" verification of identity. The SAKEM solution attempts to make this labor-intensive activity as effective as it can be. The SAKEM design anticipates increasingly sophisticated threats (i.e. it is not the result of a risk analysis that aim at a cost-efficient balance between information risks and controls).

SAKEM purpose

SAKEM is thus a procedure and a technology ([24]). Its purpose is to bootstrap a symmetric secret key shared between a new client (registrant) and a server where no prior cryptographic relationship existed before. As in the treasury management application scenario presented in the introduction, the server wishes to authenticate the cryptographic key assigned to a new client.

Server public/private key pair

For SAKEM purposes, the server needs a long-term public/private key pair for either key agreement or key transport. The trust build-up between the server and client starts with the client confidence in the server's long-term public key.

Public key trust by clients

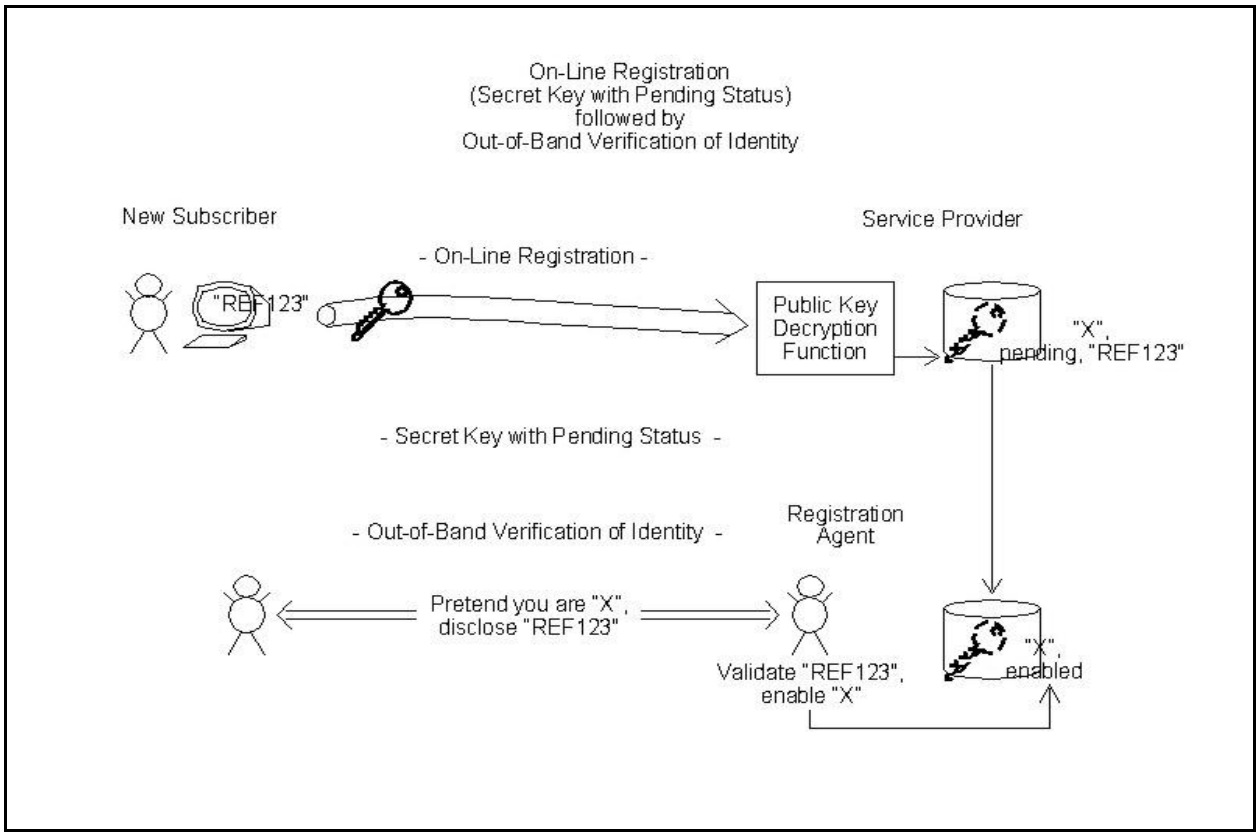
The possible procedural means assisting this trust decision by the client include embedding the server public key in a software or other packaging with a look-and-feel genuineness. In any case, the key agreement or key transport scheme should be a public key cryptosystem where protocol spoofing is difficult, e.g. a simple RSA key transport mechanism is not recommended.

Key transport or key agreement

NIST defines key transport as a "method of establishing a key whereby one of two parties (the sender) selects a value for their shared secret keying material and then informs the other party (the receiver) of that value" ([4]). If key transport is considered adequate for a SAKEM usage context, the transport goes from client to the server using the server public key for to conceal the key value. Likewise, NIST defines key agreement as a "method of establishing keying material, whereby two parties (the initiator and the responder) contribute to the value of a shared secret from which (secret) keying material is then derived."

PEKE

The author's organization developed the SAKEM procedure with the PEKE (Probabilisitc Encryption Key Exchange) cryptosystem ([25]) as either a key transport or key agreement technique. PEKE is a variant of the Blum-Goldwasser probabilistic encryption scheme ([26]) that is provably as secure as the factorization of an RSA-type modulus. It shares its security foundation with the Rabin-Williams cryptosystem ([27], [28]). Before the adoption of elliptic curve cryptography, the Rabin-Williams cryptosystem and derivatives were the most efficient public key primitives (e.g. [29], [30]). PEKE is designed to be immune to chosen ciphertext attacks. By making the PEKE initiator message an optional procedure element, PEKE provides both the key transport and key agreement functionality. The attractiveness of widely accepted technologies may justify the selection of an alternate public key cryptosystem for PEKE in the SAKEM technology. However, the NIST initiative on key management guidelines appears to move slowly and currently does not recognize the need for a key agreement scheme where a single entity has a long-term public key, as with SAKEM. In any case, the SAKEM usage of a public key cryptography primitive creates no external interoperability requirements.



On-line registration message

The SAKEM procedure is made of an on-line registration phase and the out-of-band verification of identity, with a single-use password linking the two. The on-line registration phase is implemented as a SAKEM client software component. It starts with the key transport or key agreement protocol to create a secret value shared between the client and the server. Two keys are derived from this shared secret, respectively a symmetric key used as a session key for on-line registration message protection (e.g. AES, [31], [32], in the CCM mode of operation, [33]) and the client's symmetric secret key to be authenticated for server purposes. With the key transport alternative, the on-line registration phase can use store-and-forward communications (e.g. e-mail), while the key agreement alternative needs immediate connectivity with the server systems.

On-line registration, end-users

To end-users, the SAKEM client software should look like an on-line form to be filled for registration purposes. Various client identification elements and service characteristics elements may be part of this form, plus the single-use password for SAKEM registration completion. With the growing concern with theft of identity, the disclosure of sensitive personal

identification data may be deferred to the out-of-band verification of identity.

On-line registration, network devices

In applications to field deployment of secure network devices, the SAKEM client software component is triggered during field installation or a field visit by a service technician. The user interaction is less demanding than for end-users since a device serial number or configured addressing information should be available to the SAKEM client software. Such information should be made available to the service technician and the single-use password should be agreed between the client software and its user (e.g. each one provides a portion of the password). The paperwork that keep track of field technician activities (i.e. work tickets, field trip reports) is a suitable place to record the single-use passwords, e.g. when field installations are a routine activity. In this context, the handwritten signature by the field technician becomes the basis of network device secret key authentication.

On-line phase conclusion

After the on-line registration phase is completed, the SAKEM registration procedure is still incomplete. An end-user registrant should be able to remember the single-use password and its intended purpose, i.e. the completion of registration for a given secure service. For field initialization of network devices, work tickets or field trip reports are being forwarded to the server overseeing organization.

Server processing of registration messages

Once received in the server data processing center, the SAKEM registration message is processed (reversal of the cryptographic processing done by the SAKEM client software) and then stored in a database of registration requests awaiting out-of-band verification of identity. Although the conceptual framework is relatively simple, care must be taken of the integration of SAKEM server processing to network communication facilities, database systems, and workflow management. The author's organization offers the required secure server equipment, cryptographic software, and internal control procedures documentation ([34], [35]). The target security level for these SAKEM-specific items is analogous to security requirements for the CA operations (i.e. the SAKEM server private key deserves a protection strength analogous to a CA private signature key) (e.g. [36], [37]). The server database security is a separate concern to be addressed irrespective of the initial registration strategy.

Out-of-band verification of identity

In the out-of-band verification of identity that completes the SAKEM procedure, a server's organization employee or agent is presented with the relevant client information, including data from the on-line registration message. The out-of-band channel might be a telephone conversation, a

personal visit to a branch or local office, or, as in the above example of field initialization of network devices, incoming mail processing. The registrant should reveal the single-use password for the purpose of identity verification (in the presence of a higher degree of suspicion, a *pass query* is assigned to the employee or agent for authenticating himself/herself to the registrant, hence the term *pass reply* used for the registrant's single-use password).

SAKEM procedure conclusion

If the employee or agent is satisfied with the claimed identity of the registrant and the registrant's knowledge of the single-use password, the matching SAKEM registration message should be accepted as an authenticated symmetric secret key shared with the client. Otherwise, the SAKEM registration message should be cancelled.

Conclusion

Initial key authentication

The initial authentication of some cryptographic keys is a pervasive requirement for practical security schemes based on cryptographic techniques. Many authors of security scheme descriptions assume that the reader understands the significance and implications, e.g. by referring to a trusted channel to distribute the keying material. In practice, the required procedural means are challenging as an operational burden and a mating point between technology and business processes. Procedural means for initial authenticated key distribution are seldom addressed in the literature.

SAKEM impact, client registration

The SAKEM proposal suggests a paradigm shift in client registration for secure on-line services. Instead of establishing a password with a delivery procedure supposedly reaching the intended client, new clients would apply electronically and then prove their identity out-of-band. In the new scheme, the shared secret is never exposed in the clear.

SAKEM impact, field initialization of network devices

For field-initialization of network devices, the SAKEM procedure is an infrastructure facilitation technology. It provides a structured approach to the ever-present issue of bootstrapping a security association between a network device client and a server, which can then be turned into a secure enrollment as a participant in a larger network.

Acronyms

AES Advanced Encryption Standard, the foremost symmetric cipher algorithm, adopted by NIST in 2001.

CA Certification Authority, an important entity in the PKI scheme.

CCM Counter with Cipher block chaining-Message authentication code, a mode of operation (i.e. usage rules) for symmetric cipher algorithm, e.g. AES.

NIST National Institute of Standards and Technology, an important standardization organization in the United States.

PEKE Probabilistic Encryption Key Exchange, a public key cryptography scheme for key transport or key exchange ([14]).

PKI Public Key Infrastructure, an elaborate information security scheme that was envisioned to foster ubiquitous use of public key cryptography techniques.

RFC Request For Comments, the name used for Internet standard documents.

RSA Rivest, Shamir, Adleman, the three authors of a famous public key cryptosystem that is based on the difficulty of factoring large integers.

SAKEM Secret Authentication Key Establishment Method, the scheme proposed in the present document.

TLS Transport Layer Security, an important Internet security protocol, originating from the SSL, Secure Socket Layer.

References

[1] NIST, *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, May 25, 2001

[2] Common Criteria Project Sponsoring Organizations, i.e. Canada: Communications Security Establishment, France: Service Central de la Sécurité des Systèmes d'Information, Germany: Bundesamt für Sicherheit in der Informationstechnik, Netherlands: Netherlands National Communications Security Agency, United Kingdom: Communications-Electronics Security Group, and US: National Institute of Standards and Technology and National Security Agency, *Common Criteria for Information Technology*

Security Evaluation, part 1: *Introduction and general model*, part 2: *Security functional requirements*, and part 3: *Security Assurance Requirements*, Version 2.2, January 2004.

[3] Thomas Wu, *The SRP Authentication and Key Exchange System*, RFC-2945, September 2000, http://www.ietf.org/rfc/rfc2945.txt

[4] NIST, *Recommendation on Key Establishment Schemes*, draft Special Publication 800-56, Draft 2.0, January 2003

[5] Christopher Allen, Tim Dierks, *The TLS Protocol Version 1.0*, RFC-2246, January 1999, http://www.ietf.org/rfc/rfc2246.txt

[6] Tim Dierks, Eric Rescorla, *The TLS Protocol Version 1.1*, Internet-Draft, December 2004, http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-09.txt

[7] Xiaoyi Liu, Cheryl Madson, David McGrew, Andrew Nourse, *Cisco Systems' Simple Certificate Enrollment Protocol(SCEP)*, Internet-Draft, 11 Feb 2005, http://www.ietf.org/internet-drafts/draft-nourse-scep-11.txt

[8] US patent document 5,680,458, Spelman, Jeffrey F., Thomlinson, Mattew W., *Root Key Compromise Recovery*, October 21, 1997, assigned to Microsoft Corporation

[9] US patent document 4,771,461, Matyas, Stephen M., *Initialization of Cryptographic Variables in an EFT/POS Network with a Large Number of Terminals*, September 13, 1988

[10] William E. Burr, Donna F. Dodson, W. Timothy Polk, *Electronic Authentication Guideline*, Version 1.0.1, NIST Special Publication 800-63, September 2004

[11] Carlisle Adams, Stephen Farrell, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, RFC-2510, March 1999, http://www.ietf.org/rfc/rfc2510.txt

[12] Carlisle Adams, Stephen Farrell, Tomi Kause, Tero Mononen, *Internet X.509 Public Key Infrastructure -- Certificate Management Protocol (CMP)*, Internet-Draft, February 12, 2004, http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc2510bis-09.txt

[13] European Committee for Standardization, *Cryptographic module for CSP key generation services protection profile CMCKG-PP*, CWA 14167-3:2004 E, May 2004

[14] John Kohl, B. Clifford Neuman, *The Kerberos Network Authentication Service (V5)*, RFC-1510, September 1993, http://www.ietf.org/rfc/rfc1510.txt

[15] Tom Yu, *The Kerberos Network Authentication Service (Version 5)*, Internet-Draft, 21 January 2005, http://www.ietf.org/internet-drafts/draft-ietf-krb-wg-rfc1510ter-00.txt

[16] US patent document 5,606,617, Stefanus Brands, *Secret-key certificates*, February 25, 1997

[17] Jim Shaad, *CMC Extensions: Server Side Key Generation and Key Escrow*, Internet-Draft, February 2005, http://www.ietf.org/internet-drafts/draft-ietf-pkix-cmc-archive-01.txt

[18] Michael Tuexen, Randall Stewart, Peter Lei, *Authenticated Chunks for Stream Control Transmission Protocol (SCTP)*, Internet-Draft, January 18, 2005, http://www.ietf.org/internet-drafts/draft-tuexen-sctp-auth-chunk-02.txt

[19] Pasi Eronen, Hannes Tschofenig, *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*, Internet-Draft, 17-Dec-04, http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-05.txt

[20] Florent Bersani, Hannes Tschofenig, *The EAP-PSK Protocol: a Pre-Shared Key EAP Method*, Internet-Draft, February 13, 2005, http://www.ietf.org/internet-drafts/draft-bersani-eap-psk-07.txt

[21] Carl Rigney, Allan C. Rubens, William Allen Simpson, Steve Willens, *Remote Authentication Dial In User Service (RADIUS)*, RFC-2865, June 2000, http://www.ietf.org/rfc/rfc2865.txt

[22] Carl Rigney, *RADIUS Accounting*, RFC-2866, June 2000, http://www.ietf.org/rfc/rfc2866.txt

[23] Uri Blumenthal, Lakshminath Dondeti, Randy Presuhn, Eric Rescorla, *Comparison of Proposals for Integrated Security Models for SNMP (Simple Network Management Protocol)*, Internet-Draft, February 13, 2005, http://www.ietf.org/internet-drafts/draft-ietf-isms-proposal-comparison-00.txt

[24] US patent document 6,061,791, Moreau, Thierry, *Initial Secret Key Establishment Including Facilities for Verification of Identity*, May 9, 2000

[25] Moreau, Thierry, *Probabilistic Encryption Key Exchange*, Electronics Letters, Vol. 31, number 25, 7th December 1995, pp 2166-2168

[26] Blum, Manuel, and Goldwasser, Shafi, *An Efficient Probabilistic Public-key Encryption*

Scheme which Hides All Partial Information, In Advances in Cryptology: Proceedings of Crypto'84, Springer-Verlag, 1985, pp 289-299

[27] Rabin, M.O., *Digital Signatures and Public Key Functions as Intractable as Factorization*, MIT Laboratory for computer science, TR 212, January 1979, pp 1-16

[28] Williams, Hugh C., *A Modification of RSA Public-Key Encryption*, IEEE Transactions on Information Theory, Vol IT-26, no. 6, November 1980, pp 726-729

[29] US patent document 5,299,263, Beller, Michael J., Yacobi, Yacov, *Two-Way Public Key Authentication and Key Agreement for Low-cost Terminals*, March 29, 1994, assigned to Bell Communications Research, Inc.

[30] US patent document 5,406,628, Beller, Michael J., Yacobi, Yacov, *Public Key Authentication and Key Agreement for Low-cost Terminals*, April 11, 1995, assigned to Bell Communications Research, Inc.

[31] Joan Daemen, Vincent Rijmen, *AES Proposal: Rijndael*, draft 1.1, 20/08/1999

[32] NIST, *Specification for the Advanced Encryption Standard (AES)*, FIPS Publication 197, November 26, 2001

[33] Morris Dworkin, NIST, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, NIST Special Publication 800-38C, May 2004

[34] Moreau, Thierry, *Server-side Public Key Cryptography Apparatus with Private Key Protection and Isolation from Public Networks*, Canadian patent application number 2,271,178, filed on May 6, 1999

[35] CONNOTECH Experts-conseils inc., *The SAKEM/WIRC Key Management System Design*, Document Number C003305, 2005

[36] European Committee for Standardization (CEN), *Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP*, CWA 14167-2:2004, May 2004

[37] US patent document 5,604,801, Dolan, George M., Holloway, Christopher J., Matyas, Jr., Stephen M., *Public key data communications system under control of a portable security device*, Feb. 18, 1997, assigned to International Business Machines Corporation