CONNOTECH Experts-conseils inc.

An Information Security Framework Addressing the Initial Cryptographic Key Authentication Challenges

Document Number C002693

2004/05/24

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

Abstract

The top-down information security framework uses a governing definition of information security and lists the security services in order to define *authentication*. At a lower level of abstraction, the cryptographic mechanisms are discussed, with a reminder that key management schemes (including the PKI) eventually revert to non-cryptographic means for cryptographic association establishment. Our framework introduces the SAKEM procedure (Secret Authentication Key Establishment Method), a unique scheme for providing secret key authentication precisely where an out-of-band secret key distribution would otherwise occur, when a credential service provider enrolls a new subscriber.

Document Revision History

C-Number	Date	Explanation
C002437	2004/02/24	First release
C002472	2004/03/10	Minor editorial corrections
C002693	2004/05/24	Use terminology from NIST SP-800-63
C002693		

Introduction

In a recent article [1], a new definition of information security has been suggested: *a well-informed sense of assurance that information risks and controls are in balance*. The first part refers to the benefit of information security in the perspective of high management. The second part hints at a reasonable assessment of information risks, and a proper selection of information controls. In the present article, we will discuss the contribution of cryptography to information controls, bringing into focus the initial establishment of cryptographic keys as an information control barring the "theft of identity" risk. This subject matter is a mating point between cryptography (a technology-intensive field) and generic information controls (a process-intensive field), and as such it is seldom addressed by cryptographers. In an attempt to reconcile the big picture and some detailed concepts, we make oversimplifications that a knowledgeable reader may forgive or criticize at his option.

Information Security Services

In a top-down analysis of information security, a taxonomy of *security services* is perhaps useful. Security services are still at a level of abstraction that spans the various elements of the above definition, but they are useful in positioning the diverse information controls in the global picture. The following non-exhaustive list is given here as a reminder for the wide scope of information security, in order to realistically position the potential contribution from cryptographic techniques.

A) The *confidentiality* service.

B) The *non-repudiation* service, related to the *integrity* service as discussed below.

C) The *availability* service, also referred to as *denial of service protection*.

D) The *traceability* service, based on the reliability of the application log, which is a favorite one for auditors.

E) The *replay prevention* service, which is perhaps more relevant to electronic funds transfers than to data protocol design where replay prevention is a generic engineering issue.

F) The *intractability* service appeared as an essential ingredient in electronic currency schemes where the anonymous aspect of cash transactions need to be preserved.

G) The *traffic flow confidentiality* service, which is a military intelligence concern.

Up to this point, the list of services makes no reference to cryptography. The foremost contributions of cryptography, as an information control technology, lies in the area of *confidentiality* and *non-repudiation* services (many schemes go beyond these basic services, but let's keep things simple). The introduction of technology in our top-down analysis brings some interesting refinements.

Let's start with a definition of *authentication*. If we were to qualify authentication as a security service, it would actually be a structuring one that supports other security services. Authentication is a sense of assurance that a given data element (application data element or a cryptographic key) originates from a given entity (person, organization, role of a person, automated functions of a computer server or network processor). We deliberately define authentication in a way that spans the various elements of the governing definition of information security. Other authors may use the term authentication for a cryptographic mechanism that binds a data element to a cryptographic key in the context of a non-repudiation service.

When cryptography works, it does so because it is properly implemented [2]. But even then, it merely shifts the information control focus from *application data* controls to *cryptographic key material* controls. Indeed, key management is (literally) key to cryptography! It is perhaps useful to recall that at the end of the recursive re-use of cryptographic techniques for key management functions, the user organization is left with a process-intensive information control requirement (e.g. out-of-band secret key distribution, manual master key distribution, root certificate management).

With this understanding of cryptography and authentication, we can extend the above list of security services.

H) The *privacy protection* service may be described as the confidentiality service in the context of questionable authentication of cryptographic keys.

I) Likewise, the *integrity* service may be described as the non-repudiation service in the context of questionable authentication of cryptographic keys.

J) Perhaps, the *notarization* service may be described as the traceability service in the context of adequate authentication of cryptographic keys.

Cryptographic Mechanisms

We can now turn to the more factual cryptographic *mechanisms*, which are potentially strong information controls, but standing on some shaky grounds: 1) authentication abstraction uncertainty, 2) imperfections of key management operations, 3) inadequacies of user security training and discipline, and 4) time-to-market and unit cost pressure for mass market applications. The four main cryptographic mechanisms are 1º *encryption*, 2º *digital signature*, 3º *message authentication code*, and 4º *security certificate*. The table below gives the security services provided by the mechanisms according to the authentication context. The security certificate mechanism is a digital signature applied to the data pair <public key, entity name>.

Cryptographic mechanism \ Authentication context	Adequately authenticated cryptographic keys	Questionably authenticated cryptographic keys
Encryption	Confidentiality	Privacy protection
Message Authentication Code (MAC)	Reduced non-repudiation	Integrity
Digital signature	Non-repudiation	Integrity
Security certificates	Non-repudiation of key authentication	

In the above table, the tandem digital-signatures/security-certificates is the main components of a Public Key Infrastructure (PKI). We position the old-fashioned MAC mechanism almost at par with a PKI, with the following justification:

I) The PKI technology is so effective in shifting the information control focus to the top-level Certification Authority (CA) operations, that the CA liability exposure became a pervasive concern, and the PKI initiatives are nowadays limited to the closed PKI model, where a central organization trusts only itself.

II) The end-user education challenge was not met for the following reasons:
   i) the emphasis on security certificate usage restrictions (motivated by the CA limitation of liability) obscured the critical need to preserve the long-term secrecy of the end-user private key [3],
   ii) any mass market PKI initiative is plagued by the zero cost target for private key storage hardware in the end-user environment, and
   iii) the Certificate Revocation List management adds an unprecedented level of complexity in any information security scheme [4].

III) Concurrent with the collapse of the .com economy, came the realization that no open public key infrastructure would ever emerge to support ubiquitous authentication of cryptographic keys that the technology promised [5]. There remains the closed PKI alternative, where an organization relies solely on its own CA operations to support non-repudiation.

According to our analysis, the non-repudiation service may be provided with the old-fashioned MAC mechanism. The fact that the verifying party in the MAC mechanism does not cheat with the secret key database to forge transactions is equivalent to the fact that the CA in a closed PKI scheme operates with due diligence and provides reliable logs of certificate issuance and revocation. In either case, we whish to stress the cryptographic key authentication as the critical factor for effective non-repudiation service. Indeed, a security certificate provides no security service in the context of questionably authenticated cryptographic keys.

Initial Key Establishment

In most cryptographic scheme descriptions, initial key distribution is achieved by "out-of-band" means. In technical or commercial documentation, initial key distribution coverage is usually even more elusive. For instance in the case of a PKI, initial key distribution is a two-fold process for each end-user: some procedural provision should be made for root CA public key recovery (e.g. [6]), and the security certificate issuance must be somehow protected against various attack scenarios. On this last subject area, we couldn't find a satisfactory reference publication. The only reference containing a "proof of possession" specification is an Internet standard for PKI certificate management protocols that explicitly requires "out-of-band distribution of Initial Authentication Key" for certificate issuance [7].

In practice, all sorts of activities seem to qualify as out-of-band key distribution, from e-mail delivery to dual custodian key component key transport, and also diverse schemes where a token or device is initialized before its handing out to the subscriber. In summary, there is a commonality of issues surrounding the issuance of initial cryptographic keys, irrespective of the security mechanism (encryption, MAC, or digital-signature/security-certificate). At least for high risk applications, the prevailing current practice appears inadequate in this respect.

Let's go back to the definition of information security. In view of inadequate controls of initial cryptographic key establishment, mere privacy and integrity protection are afforded when confidentiality and non-repudiation would appear necessary. Empirically, a large sector of the information security works this way, and we propose the following analysis:

a) the protection downgrade is either not recognized or ignored,
b) few security incidents are documented against this protection downgrade, or
c) it is acceptable due to the level of information risks.

Note that the operating cost issue is not stated, since it is part of the "balance" portion of the governing definition. However, the growing concern about the theft of identity may change the

item b) above.

For sake of completeness the review of initial cryptographic key security should mention another basis for long-term key authentication. Key authentication being a sense of assurance that a given cryptographic key originates from a given entity, a different understanding of "entity" creates a situation where the repetitive use of a key reinforces the authentication assurance. That is to say, the usage history of a key, being representative of entity behavior, is a possible basis on which key authentication might be considered adequate. Without further analyzing this view, we should observe that the PGP web of trust model operates on this principle combined with the non-repudiation transitivity offered by the digital signature mechanism [4].

SAKEM, Secret Authentication Key Establishment Method

We designed SAKEM as a means to authenticate secret cryptographic keys by a central organization (service provider), keeping an eye on operation costs, but without sacrificing security. We use the terminology introduced by the NIST special publication 800-63 (in draft form) [8]. This publication is a welcome initiative in that the procedural aspects of the identity proofing and registration procedures are covered from a global perspective. The service provider procedures are effected partly by a credentials service provider (CSP) and partly by a registration authority (RA), which may two different entities, or a single one fulfilling the two roles.

The usual process for initial key establishment is depicted in figure 1. It is an obvious sequence of activities. The new subscriber (an end-user with whom the CSP has no prior relationship) requests an enrollment from the RA and presents the expected identity proof. Presumably, the RA verifies the new subscriber's identity, and this verification effectiveness is inescapably based on human attention and judgement (the SAKEM alternative can't change this). Once the decision is made to grant the enrollment request, the CSP or RA grants the access permission, and sends the secret key to the subscriber's computing environment, by an "out-of-band" channel.

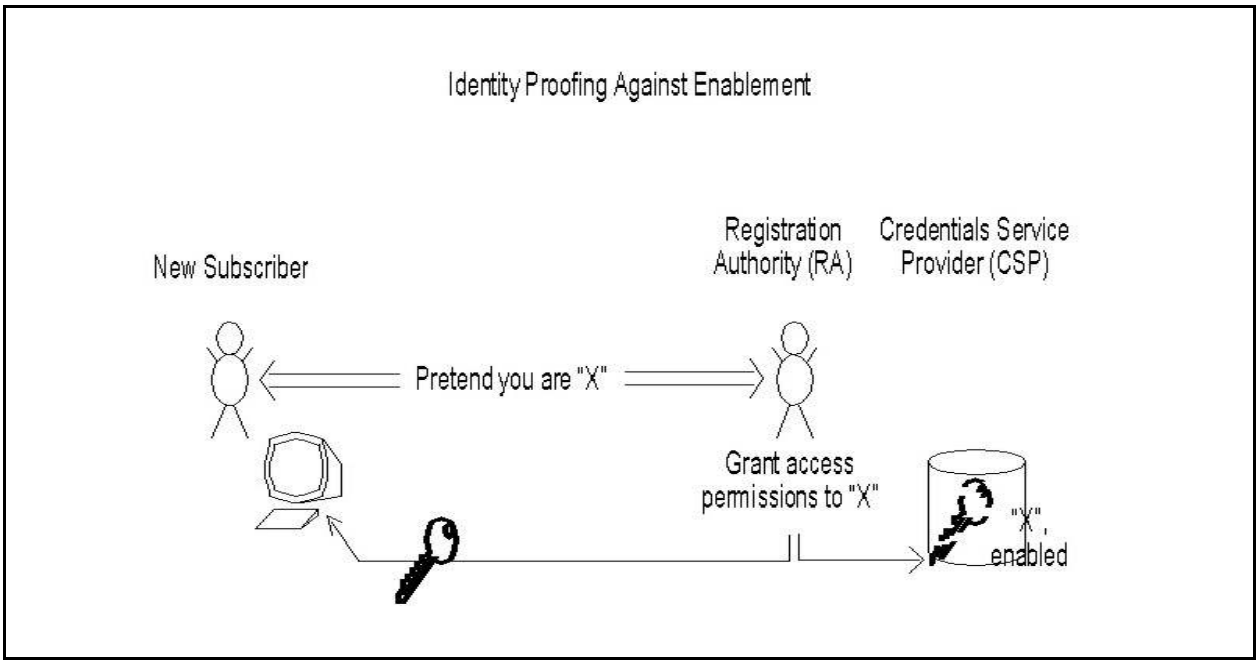

Figure 1) Usual process for initial key establishment

The SAKEM procedure, depicted in figure 2, slightly changes the new subscriber sequence of activities, streamlines the CSP/RA operations, replaces the out-of-band channel by public key encryption, and separates the registration duties by the CSP/RA [9]. In the first step, the new subscriber goes through an on-line registration step, during which the secret key is set-up in the new subscriber computing environment and in the CSP database. In a second step, the new subscriber presents the expected identity proof to the RA who verifies the new subscriber's identity. The two steps are linked together by a short-lived registration reference ("REF123" in the figure 2) and the "pending" status affixed to the secret key in the CSP database while it awaits the subscriber identity confirmation by the RA. The short-lived reference is a secret that can be remembered by a human.

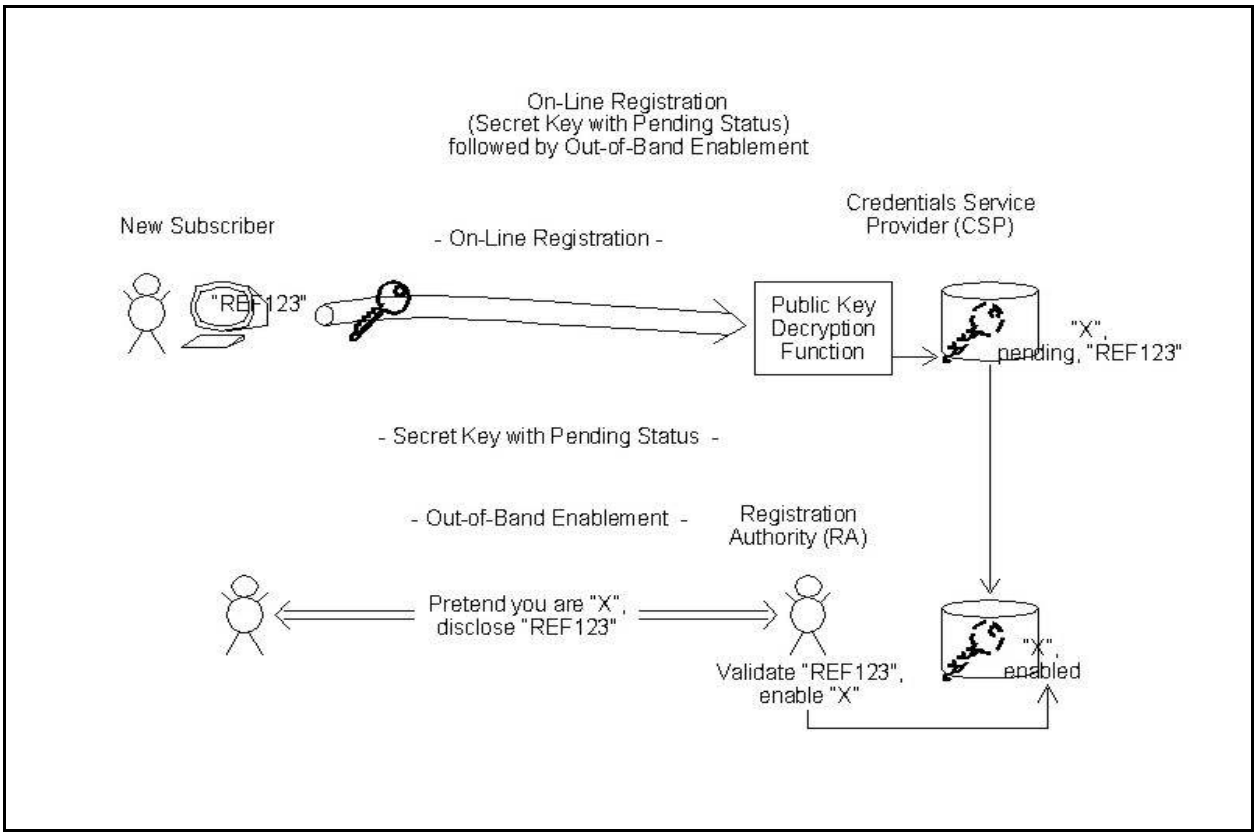

Figure 2) The SAKEM procedure

What are the application areas for the SAKEM procedure? Here are a few highlights:

- For the high risk applications where the operational burden of manual key distribution is a concern, an alternative like the SAKEM procedure should be considered.
- For field initialization of network devices, the new subscriber's role can be fulfilled by a field technician, and the identity verifier role can be fulfilled by a security officer, providing a unique separation of duties in a secret key distribution scheme that do not expose the secret key.
- Some mass market applications experience a significant fraud rate despite a low average transaction value, e.g. in the mobile telephony business. The SAKEM procedure brings a paradigm shift in the user registration procedures. Perhaps it is suitable as a countermeasure against some attack scenarios on the mobile user registration process.

The list of potential applications for SAKEM might seem endless. However, the initiation of a cryptographic association is a field encumbered by a wide range of protocols and procedures, often superimposed on existing networks and business operations, and the authentication effectiveness is seldom recognized as an essential system requirement. Instead, automated authentication re-use is often suggested without explicitly tying it to the original authentication adequacy (e.g. [10]).

The SAKEM proposal has not yet been brought to a fielded application, mainly due to the momentum towards an open PKI deployment (ubiquitous and seamless information security) that occurred until the collapse of the .com economy. Nowadays, the SAKEM benefits with regards to security and operating efficiency should appeal to an era where information security priorities are more tangibly identified.

Conclusion

In this paper, we attempted to position the original SAKEM proposal in a structured analysis of the information security sector and the contribution of cryptographic techniques to distributed security applications. We started with a governing definition recently proposed to reconcile the high level management view with the information controls (not limited to cryptographic techniques) and the information risks. If the cryptographic controls are to be effective in providing security services, it is critical to adequately authenticate the very initial keys used in cryptographic mechanisms. We argued that the PKI certificate management does not depart significantly from prior techniques in this respect.

The SAKEM procedure is a unique scheme for providing secret key authentication precisely where an out-of-band secret key distribution would otherwise occur, when a service provider enrolls a new subscriber. As such, the SAKEM scope spans beyond the traditional limits of cryptographic protocol schemes to include some of the operational tasks associated with a new subscriber enrollment. This paper achieved its goal if the reader can relate the SAKEM procedure to other schemes, protocols or procedures aiming at similar or seemingly similar goals. A review of the SAKEM procedure details is outside the scope of this paper.

References

[1] James M. Anderson, *Why We Need a New Definition of Information Security*, Computers & Security, vol 22, no. 4, May 2003, 2003, pages 308-313.

[2] Anderson, Ross J., *Why Cryptosystems Fail?*, Communications of the ACM, November 1994

[3] Biddle, C. Bradford, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace*, San Diego Law Review, Vol 34 (1997), issue 3, pp 1225-1246

[4] Ed Gerck, Ph.D., *Overview of Certification Systems: X.509, PKIX, CA, PGP & SKIP - Do you understand digital certificates? Do you know what they warrant?* THE BELL, 2000, revised on 18.July.00., http://www.thebell.net/papers/certover.pdf

[5] Civics.com (Daniel Greenwood?), *Compilation of Resources Regarding Difficulty With PKI*, http://www.civics.com/PKI/

[6] US patent document 5,680,458, Spelman; Jeffrey F.and Thomlinson; Matthew W., *Root key compromise recovery*, October 21, 1997, (application no. 555697, November 14, 1995)

[7] C. Adams, S. Farrell, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, Internet Network Working Group, RFC2510, March 1999

[8] William E. Burr, W. Timothy Polk, and Donna F. Dodson, *DRAFT Recommendation for Electronic Authentication*, National Institute of Standards and Technology, NIST Special Publication 800-63, January 2004

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

[10] David P. Jablon, *Strong Password-Only Authenticated Key Exchange*, ACM Computer Communication Review, vol. 26, no. 5, Oct. 1996