ON THE USE OF "QUALIFIED" DIGITAL SIGNATURES

Maurizio Adriano Strangio
Department of Mathematics, University of Rome "Roma Tre", Italy

Keywords: Qualified Digital Signatures, Key Agreement Protocols.

Abstract: The European Commission Directive 1999/99/EC aims to provide a community-wide framework for the use of electronic signatures and thus for promoting electronic trade and communication among the member states. The directive introduces the notion of "qualified" digital certificates as a means to maintain legal effects of digital data that are analogous to those of paper-based signatures. To this end, proofs of (physical) identity and possession (of the private key) are fundamental requirements that must be fulfilled by the requester during the public key enrollment process.
Digital signatures are often employed as secure buildings blocks in key agreement protocols that use public key authentication. The need for the rigorous analysis of such protocols has recently emerged; there are currently several formal models of distributed computing that may serve for this purpose. However, we point out these models employ rather trivial or unpractical approaches in the modeling of the procedures and policies employed by certification authorities.
We believe that usage of qualified certificates not only should represent the standard practice for CAs in order to sustain secure electronic commerce (and in general all forms of secure communication) but also represents the first step towards the domain of a global PKI.

1 INTRODUCTION

Symmetric key algorithms have a troublesome shortcoming — the need to generate and distribute a secret key to the parties who wish to privately communicate. Furthermore, keys must be exchanged prior to any communication by making use of a (out-of-band) secret channel and not via a public network.

With public key cryptography, in a network of n principals, each party needs only to distribute a public key to her $n-1$ peers so the total number of keys to manage is $O(n)$, rather than $O(n^2)$.

However, with asymmetric key algorithms public keys can be easily exposed (since they are delivered in unencrypted form) therefore a principal using the wrong key may be totally unaware that a malicious party is posing as her intended peer. As the result, public keys must be certified in a separate process prior to any communication, possibly by a trusted third party; for the parties willing to communicate this is logically equivalent to having an authenticated channel available to distribute the public keys in order to receive assurance of each others purported identity.

In practice, this service is provided by a Public Key Infrastructure (PKI) which is an arrangement that entails a trusted third party (a.k.a. certification authority — CA) fulfilling a notary function by binding the public key (and a set of informative attributes) to the owner of the corresponding private key. The outcome of the process is a digital certificate (e.g. X.509v3), signed by the authority itself, that provides undisputable evidence of the true identity of the principal holding the private key/public key pair.

While this approach is technically straightforward, the management (e.g. operation and funding) of a PKI can become quite intricate (see (Ellison and Schneier, 2000) for an overview of the difficulties that may be encountered) so that the public key validation process may be almost as difficult as distributing secret keys (after all symmetric key cryptography has been profitably employed since the era of Ceasar).

Whether a CA may be regarded as trustworthy (which ultimately is a decision of the relying party) is a major concern and is not just a matter of considering certain distinguishing elements such as the reputation or the nationality of the CA. It turns out that there are other requirements that must be satisfied and often these are not clearly stated in the CA

Adriano Strangio M. (2008).
ON THE USE OF "QUALIFIED" DIGITAL SIGNATURES.
In *Proceedings of the International Conference on e-Business*, pages 334-338
DOI: 10.5220/0001909203340338
Copyright © SciTePress

policies (e.g. in the Certification Practice Statements — CPS) or, even worse, not even completely understood. For this reason, in some countries (e.g. Italy) there are government agencies entitled to perform the final accreditation of CAs (which are also subjected to periodic inspections to verify full compliance with the law).

In fact, the main thesis of this paper is that a "physical proof-of-identity" and "proof-of-possession" are both mandatory to maintain the legal status of digital signatures. With a physical proof-of-identity the certificate requester must provide corroborative evidence of her identity (e.g. an id-card) in a "face-to-face" registration procedure at the registration authority (RA). With a proof-of-possession the subscriber must prove he exerts (exclusive) control over the private key corresponding to the public key undergoing the certification.

Although the "physical" identification process is often perceived as an unduly burden by most subscribers (although it is essentially identical to applying for a driving license) it is beneficial for a number of reasons:

- it discourages from making use of PKIs for criminal activity;
- facilitates law enforcement agencies in the prosecution of the crimes related to signature/encryption schemes (e.g. identity theft, fraud);
- is also valuable for assessing the trustworthiness of individuals.

On the one hand, the proof-of-possession requirement has been the subject of many discussions (see (Asokan et al., 2003; Lauter and Mityagin, 2006)) with the majority of PKI standards firmly encouraging its use (observe that when the CA generates the public/private key pairs this requirement is immediately fulfilled). On the other hand, many CAs will issue certificates offering different levels of identity assurance; a physical proof-of-identity is required for the certificates that are used in applications that need to establish the purported identity of the subscriber with certainty (e.g. commercial transactions); this is opposed to certificates issued with email addresses used as identification credentials (which are suitable for non critical applications).

However, often an explicit indication of how the subscriber was identified is omitted from the certificate attributes thus opening subtle vulnerabilities in its use (the relying party may unwillingly omit to perform any validity checks).

We stress that a proof-of-possession merely implies that the applicant has access to the private key corresponding to the target public key; therefore a physical proof-of-identity is essential for the legal recognition of digital signatures.

CA policies often refer to the PKCS#10 standard (PCKS#10v1.7, 2000) which describes a syntax for certification requests; an entity applying for a certificate may be prompted by the RA to digitally sign an electronic "certificate request" that will be subsequently conveyed to the CA for the final certificate handout. Such an arrangement subsumes a proof-of-possession. Surprisingly, the standard also includes the provision for requests using paper forms; this implies that CAs should define alternative means in their policies for the requester to prove knowledge of the private key.

2 DIGITAL CERTIFICATES IN THE EUROPEAN COMMUNITY

The European Commission Directive 1999/99/EC (European-Parliament, 1999) aims to provide a community framework for the use of electronic signatures and thus for promoting electronic trade and communication among the member states.

In particular, the legal recognition of electronic signatures entails the use of *advanced electronic signatures* based on "qualified certificates", which are created by secure (signature-creation) devices (e.g. tamper-proof standard-compliant devices such as smart cards holding the private key), to ensure they:

(a) satisfy the same legal requirements of hand-written signatures on paper-based data (refer to the definition of advanced electronic signature in the Directive);

(b) are admissible as evidence in a court of law.

The majority of European member countries have already embodied the directive in their legal systems (civil laws).

Qualified certificates are certificates that comply with the rules contained in Annexes I and II of the aforementioned Directive and appear to satisfy both the proof-of-possession (Annex I, letter (e)) and proof-of-identity (Annex I, letter (c)) requirements as we discussed in the preceding section.

Under such arrangements we call the resulting certificates "strong qualified certificates"; as opposed to "weak qualified certificates" which may be supplied by CAs that do not strictly comply with both the above requirements (e.g., consider a CA performing a proof-of-identity by means of an on-line zero-knowledge identification protocol).

3 KEY ESTABLISHMENT PROTOCOLS THAT USE DIGITAL SIGNATURES

Digital signature schemes (and other public key encryption schemes) are often employed as secure building blocks in key establishment protocols that use public key authentication for the purpose of ensuring the parties involved in the communication that the session key was established with the intended peer and not with an impostor. Once a session key is available, the data exchanged is authenticated and undisclosed against third parties thus allowing secure communications over an insecure network.

Traditionally, cryptographic protocol security has been a matter of perceived confidence supported by heuristic proof arguments and by the protocol surviving many years of public scrutiny. More recently, the approach has changed and the priority has switched to developing formal proof frameworks. In this context, a main line of research employs complexity-theoretic models for distributed network computing and is dedicated to key establishment protocols (Bellare and Rogaway, 1993; Blake-Wilson and Menezes, 1998; Shoup, 1999; Bellare et al., 2000; Canetti and Krawczyk, 2001; LaMacchia et al., 2006; Diffie et al., 1992). Such models employ both private and public key cryptographic techniques.

In the above models most of the fine level details of PKIs are abstracted away; while in principle this is a reasonable approach (we already mentioned that PKIs are an intricate subject on their own) we often see that important topics such as the key registration procedures and policies employed by CAs are disregarded by many authors. We believe that such issues are not only tightly related to the correct operation of the protocol but may also eventually lead to (legal) disputes among the participants and therefore must be appropriately settled.

As a starting point for our discussion, let us recall three public key registration procedures commonly encountered in the literature (LaMacchia et al., 2006):

a. *Honest key registration*. All parties (including those controlled by the adversary) follow the key generation procedures honestly and register the resulting public keys before engaging in any communications. The adversary can corrupt parties only after key registration has completed;

b. *Proof-of-possession*. An authority performs some validity check upon public key registration. In particular, a party is required to prove knowledge of the corresponding secret key. The adversary can register public keys for corrupted parties at any time;

c. *Arbitrary key registration*. Parties can register arbitrary public keys (even the same key as some other party) without any validity checks. The adversary can register public key for corrupted parties at any time.

We comment that case c. is unrealistic since it is extremely unlikely that a CA will ever accept to enroll public keys for which the requester has not provided any validity check; the minimum requirement is verifying the identity of the applicant.

Item a. exemplifies the behavior one would normally expect from honest principals holding valid certificates. The case of interest here is the compromise of the private key of a principal whether or not he is aware of this fact (the adversary may be able to subtly obtain a copy of the private key).

The proof-of-possession requirement invoked by item b. is not sufficient to achieve adequate levels of security (as discussed above); we have already pointed out that without a proof-of-identity CAs will not issue certificates. We now elaborate further on this point.

Lauter and Mityagin (Lauter and Mityagin, 2006) have recently presented protocol KEA+ that, as opposed to the original version (KEA), is resilient to unknown key share (UKS) attacks; as a countermeasure, they suggest to include the identities of the protocol participants as arguments of the key derivation function (KDF) and also claim that the above countermeasure avoids the need for a proof-of-possession.

Recall that a UKS attack involves a (man-in-the-middle) adversary, posing as a legitimate party (say C) in a protocol run between honest parties (say A and B), that is able to convince one party (e.g. A) to accept her identity (C) while the peer (B) is unaware of this fact (i.e. B thinks he's interacting with A). This vulnerability is regarded of interest whether or not the adversary is able to have the attacked party accept a chosen session key.

We believe there are two issues that are overlooked in their arguments. Firstly, the adversary must provide a valid proof-of-identity; therefore, unless she is willing to reveal her true identity (otherwise she must be able to perfectly disguise herself and also offer a counterfeit id card — indeed a non trivial task), she may be liable of being legally pursued for her actions in a court of law. Observe also that the (physical) proof-of-identity policy rules out the well known online UKS attack described by Kaliski (Kaliski, 2001) against the MQV protocol (Law et al., 2003) (notice that in this attack the adversary is able to have the target party accept a chosen session key).

Secondly, the lack of a proof-of-possession (albeit

not being necessary for a protocol to resist UKS attacks) implies loss of the non-repudiation property for digital signatures; at a later time the signer can eventually deny having participated in the protocol run (and therefore having established a particular session key with a peer).

We may conclude that the KEA+ protocol (and many others alike) are not suitable for electronic trade and commerce and at best can be used within the realm of a corporate domain for the exchange of data between employees (the proof-of-possession would be satisfied anyway since the keys are generated and managed in house).

From the above remarks we see that the primary sources of concern derive from the legal implications involved in electronic data processing facilities (which constitute the underlying principles of the European Directive).

The lessons learned are twofold:

- strong qualified certificates are necessary to prevent legal disputes;
- if legality is not a concern peers may use weak qualified certificates.

Therefore, relying parties must be able to verify certificate policies of the CA to determine whether the certificates are suitable and trustworthy for a particular application.

As a consequence, CAs should also have clearly stated policies for appropriately setting certificate attributes; for example, in strong qualified certificates the X.509v3 Key Usage extension (RFC3280, 2000) should always specify only one use for the public key (namely for signature validation) and have the non repudiation bit asserted.

We mention the recent attempt of Boldyreva *et al* (Boldyreva et al., 2007) to set out rigorous models of the public key enrollment process with a CA. In particular, they show that a simple challenge-response interactive protocol suffices to fulfill the proof-of-possession requirement. Notice that a fundamental assumption in their work is the existence of an authentic channel between the user and the CA; although (as the authors admit) it would be otherwise difficult to establish any reasonable security claim this hypothesis enormously reduces the practical usefulness of the registration protocols (e.g. running it on an open network environment is risky — similar arguments apply to the proof-of-possession protocols found in the technical literature for the Internet (RFC2875, 2000)). As a possible enhancement to the registration protocols, one may consider the CA assigning a unique transaction key TK to the subscriber when the physical proof-of-identity is performed; the TK may be used only once either as a shared session key (provided it is cryptographically strong enough — say, at least 128 bits) or as an access token to be included as an argument of the registration protocol on the user side (and verified by the CA) thus providing an authenticated communication channel.

4 CONCLUSIONS

In this paper we have (re)affirmed the need for CAs to require mandatory proofs of identity and possession (of the private key) from subscribers requesting digital certificates for public keys in order to preserve the legal status of the associated signature schemes. We have also reviewed the notion of qualified certificates as introduced by the European community directive 1999/99/EC (European-Parliament, 1999). As far as electronic documents are concerned (e.g. contracts) the directive says that all member states should ensure that advanced electronic signatures (i.e. signatures that are linked to qualified certificates) must be given the same legal effect as paper-based signatures and are thus form valid evidence in court trials.

We have also pointed out that formal models of distributed computing, where the security of key establishment protocols using public key authentication is evaluated, often adopt a rather trivial approach when considering public key enrollment procedures.

Our main thesis is that large-scale CAs (offering national or international cross-border services) should only offer qualified certificates (with the appropriate proofs established) whether they are relative to digital signatures used to sign documents or employed as building blocks in key establishment or other cryptographic protocols. Other types of certificates, which we have broadly classified as weak qualified certificates, only grant a limited degree of security (assurance) with no legal effects and can be eventually used in particular domains (e.g. the PKI used in a home-banking system).

Although (in principle) one could choose the appropriate certificate depending on the application (among those offered by a CA) there would be significant benefits if all the players involved could assume that certificates delivered an equivalent degree of assurance rather than having to rely on non-standard policies. To this end, it would be desirable that strong qualified certificates be adopted as a universal standard for digital signatures, thus delivering further impulse to the development of interoperable world-wide PKIs.

ACKNOWLEDGEMENTS

The author is grateful to the reviewers for their helpful comments and suggestions.

REFERENCES

Asokan, N., Niemi, V., and Laitinen, P. (2003). On the Usefulness of Proof-Of-Possession. *Proceedings of the 2nd Annual PKI Research Workshop*, pages 122–127.

Bellare, M., Pointcheval, D., and Rogaway, P. (2000). Authenticated Key Exchange Secure Against Dictionary Attack. *In Proceedings of EUROCRYPT 2000*, LNCS 1807:139–155.

Bellare, M. and Rogaway, P. (1993). Entity Authentication and Key Distribution. *In Proceedings of CRYPTO 1993*, LNCS 773:232–249.

Blake-Wilson, S. and Menezes, A. (1998). Entity authentication and Authenticated Key Transport Protocols Employing Asymmetric Techniques. *Security Protocols - 5th International Workshop*, LNCS 1361:137–158.

Boldyreva, A., Fischlin, M., Palacio, A., and Warinschi, B. (2007). A Closer Look at PKI: Security and Efficiency. *Proceedings of PKC 2007*, LNCS 4450.

Canetti, R. and Krawczyk, H. (2001). Analysis of Key Exchange Protocols and Their Use for Building Secure Channels. *Advances in Cryptology-EUROCRYPT 2001*, LNCS 2045:453–474.

Diffie, W., van Oorschot, P., and Wiener, M. (1992). Authentication and Authenticated Key Exchange. *Designs, Codes and Cryptography*, 2:107–125.

Ellison, G. and Schneier, B. (2000). Ten risks of PKI: What you're not being told about Public Key Infrastructure. *Computer Security Journal*, 16(1):1–7.

European-Parliament (1999). Directive 1999/99/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

Kaliski, B. (2001). An Unknown Key Share Attack on the MQV Key Agreement Protocol. *ACM Transactions on Information and System Security*, pages 36–49.

LaMacchia, B., Lauter, K., and Mityagin, A. (2006). Stronger Ssecurity of Authenticated Key Exchange. *http://eprint.iacr.org/2006/073*.

Lauter, K. and Mityagin, A. (2006). Security Analysis of KEA Authenticated Key Exchange Protocol. *Proceedings of PKC'06*, LNCS 3958:378–394.

Law, L., Menezes, A., Qu, M., Solinas, J., and Vanstone, S. (2003). An Efficient Protocol for Authenticated Key Agreement. *Designs, Codes and Cryptography*, 28:119–134.

PCKS#10v1.7 (2000). Certificate Request Syntax Standard. RSA Laboratories.

RFC2875 (2000). Diffie-Hellman Proof-of-Possession Algorithms. Network Working Group.

RFC3280 (2000). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List CRL Profile. Network Working Group.

Shoup, V. (1999). On Formal Models for Secure Key Exchange. Technical Report RZ 3120, IBM Research.