Lightweight Certificates
– Towards a Practical Model for PKI

Łukasz Krzywiecki¹, Przemysław Kubiak¹, Mirosław Kutyłowski¹,
Michał Tabor²,⋆⋆, and Daniel Wachnik²

¹ Faculty of Fundamental Problems of Technology, Wrocław University of Technology
² Trusted Information Consulting, Warsaw
{miroslaw.kutylowski,lukasz.krzywiecki,
przemyslaw.kubiak}@pwr.wroc.pl,
{michal.tabor,daniel.wachnik}@ticons.pl

Abstract. We present a concept for Public Key Infrastructure based on certificates that are not understood as a guarantee of Certification Authority for unconditional authenticity of the data contained in the certificate. As liability of CA is a source of cost barrier for widespread use of PKI services, we concentrate on cost-efficient solutions. At the same time we formulate requirements that fill the security gaps of the traditional PKI. We present exemplary technical solutions that witness feasibility of these requirements.

Keywords: public key certificate, PKI, trust management, authentication, Schnorr signature.

1 Introduction

Asymmetric cryptography provides strong methods for proving that certain actions (like signing a document, remote authentication) are performed by a holder of a secret key related to a certain public key. However, for real life applications we have to link the holder of the secret key with a physical person. The purpose of PKI (Public Key Infrastructure) is to develop a framework, in which we can derive this linking information. The standard way is to issue digital certificates. Standards, such as X.509, help very much to develop software integrating cryptographic tools, however do not provide comparable security guarantees as a lot depends on purely procedural issues.

1.1 Traditional PKI Approach

The standard way of linking a physical person with a certificate is as follows:

– we assume that each person holds documents confirming identity, in most cases these are personal ID documents (personal ID documents issued by authorities, or less official ones like driving license, social security card, etc.). A silent assumption is that this system is secure.

⋆ This research has been partially supported by Foundation for Polish Science, Programme MISTRZ.
⋆⋆ Corresponding author.

© Springer-Verlag Berlin Heidelberg 2012
There are Certification Authorities (CA) which issue certificates and which are obliged to fulfill many strict conditions.

<table>
<thead>
<tr>
<th>Actors</th>
<th>: person ( U ), certification authority CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>: a public key ( P ) of ( U )</td>
</tr>
<tr>
<td>Output</td>
<td>: certificate of the form “( P ) is a public key of ( U )” signed by CA</td>
</tr>
</tbody>
</table>

1. \( U \) states a request for a certificate for key \( P \) the request is signed with the private key corresponding to \( P \)
2. CA runs a procedure verifying that the request comes from \( U \)
3. CA verifies the signature of the request with public key \( P \)
4. If the outcome of verifications is positive, then CA issues a certificate for \( (P, U) \)

**Algorithm 1.** Issuing a certificate - top level description

The process of issuing a certificate is described by Algorithm 1. The process mimics issuing documents like passports by public authorities. In most cases verification of the requester must be performed by personal appearance at a registration point of CA. One notable exception is the system of German personal identity cards, where this personal contact phase is overtaken by the authorities: the personal appearance occurs when the Personalausweis is given to the citizen. The protocols implemented on the ID card enable CA to check that the certificate request is coming from a personal ID document of the person declared in the request and that the correct password has been used.

The fundamental assumptions for usage of such certificates are as follows:

- a person using a certificate can entrust the certificate and is not obliged to make any precaution steps (except for checking the current status of the certificate),
- if the certificate contains false information, CA is responsible for damages and liable to make compensations.

So far, the traditional PKI model failed as a business model despite all efforts of the European states to enforce widespread usage of digital signatures. In the next subsections we name some basic reasons for this situation.

**Economic Issues.** The running costs of CA as well as their business risk are to be compensated by the fees paid by the owners of the certificates. As issuing a certificate is a one-step service and there is no control over the actual usage of the certificate, **the only feasible payment policy is to charge per certificate.** In order to secure continuous income for CA (and for some security reasons as well), the certificates have limited validity period. The major problems for such a business model is that

- a user has to pay a quite high entry price, while initially he may expect to use the certificate just a few times (at least in the first years)

There is a business deadlock: it makes no sense to buy a certificate if there are no services available, and there is no reason to build services, if the users are missing. Public administration may attempt to create such a market, but due to the cost issues usually the systems are downgraded to match justified requirements or they are not built at all.