Computers & Security (2004) **23**, 300—311

Computers & Security

www.elsevier.com/locate/cose

Formal support for certificate management policies

Victoria Ungureanu

Department of MSIS, Rutgers University, 180 University Avenue, Newark, NJ 07102, USA

Received 30 September 2003; revised 23 January 2004; accepted 11 February 2004

KEYWORDS
Certification;
Revocation;
PKI;
Certificate management policy;
Policy formulation;
Policy enforcement

Abstract Traditionally, creation and revocation of certificates are governed by policies that are carried manually, off-line, by trusted agents. This approach to certificate management is appropriate for many current applications, where these policies cannot be verified automatically (e.g. require verification of non-digital credentials). But it is expensive, time consuming and error-prone for the growing class of applications where certificate management policies can be formalized and carried out automatically. We argue that, in these cases, creation and revocation of certificates could be viewed as any other on-line service available in a system. Access to these particular service instances could be regulated much in the same manner as file access or resource allocation.

This paper proposes a formulation for certification and revocation policies, and a framework for their support. In this framework, certificate management policies are enforced by generic policy engines, wrapped around certification authorities and revocation servers. The proposed framework is easy to deploy, requiring no modifications of current public-key infrastructure (PKI). Moreover, we show that this framework is quite affordable, even in its present, experimental stage.

Introduction

Certificates, by which we mean digitally signed credentials of some sort, are increasingly used for authentication. This is in part due to the advent of electronic commerce which requires means for establishing trust between parties which are physically distant from each other. And it is in part due to the fact that the use of traditional password schemes may be problematic in large, distributed settings.

To date, several certificate frameworks (Ellison, 1999; Kent, 1993; Zimmermann, 1995) and revocation mechanisms (Iliadis et al., 2000; Stubblebine, 1995; Wright et al., 2001) have been proposed and extensively studied. What interests us here is an orthogonal aspect of certificate management, which has received considerably less attention, namely the formulation and enforcement of policies governing certification and revocation.

E-mail address: ungurean@research.rutgers.edu.

0167-4048/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.02.001

Certification

A certificate is signed on behalf of an organization by a *certification authority* (CA) if a number of provisions are met. Typically these provisions, which are specified by a Policy Certification Authority (PCA), are verified manually, off-line, by trusted agents. A CA serves a request to create a certificate only if the request is made by an agent trusted to carry out the terms of the PCA (Netscape certificate management system; RSA Keon: certificate authority).

Such an approach is indeed necessary if a PCA cannot be verified automatically—for example, if a PCA requires non-digital credentials, like birth certificates, driver's licenses, or academic diplomas. However, in the many cases when the PCA terms can be verified automatically, such enforcement of policies is time consuming, expensive and error-prone.

The drawbacks of an entirely manual approach towards certification can be illustrated by the following example. In business-to-business (B2B) e-commerce supplier-enterprises often require that purchase orders from their clients are signed by CAs established by the respective client-enterprises (Ludwig et al., 2000). From the supplier point of view, this requirement has several important benefits, including: (a) it ensures that a purchase order (PO) is valid, and (b) it makes PO validation simple, in that only one signature needs to be verified. From the client-enterprise point of view, this requirement calls for the signing of every PO. But if every little purchase is manually verified by a designated authority, the daily routine of a company, which makes a large number of purchases, is bottlenecked.

In practice, there are cases when compliance with PCAs could be verified automatically. For example, consider a large, geographically distributed company, called ACME, which is required by some of its suppliers to certify POs. Suppose further that ACME's PCA regarding PO certification states that only duly appointed purchase-officers may issue POs. If the status of purchase-officers is established by digital credentials, this PCA can be verified automatically, thus making purchasing considerably more efficient.

Revocation

Certificates might become invalid for various reasons and should be revoked. For example, in the scenario presented above, a purchase-officer might lose or otherwise compromise his private key, or he might leave the company. Most revocation mechanisms rely on the existence of *certificate revocation lists* (CRLs) maintained by trusted revocation servers. In these mechanisms, revocation is carried out as follows: the certificate owner, or another designated authority, sends the server a signed message identifying the certificate to be revoked (AT&T access certificate for electronic services; Netscape certificate management system; Wright et al., 2000). Upon receipt of the message, the revocation server updates its CRL and disseminates the information.

But, relying on the certificate owner for revocation is problematic because the owner can be entrusted to report an invalid certificate only in a limited number of cases. For example, in the ACME scenario, one cannot rely that a purchase-officer revokes his certificate when he leaves the company. And requiring that each certificate be revoked by a designated agent, usually a person, is an expensive, error-prone process. An alternative to revocation is issuing certificates with short validity periods (Rivest, 1998). But this solution requires frequent renewal of certificates, and thus is computationally expensive if the number of certificates issued on behalf of an organization is large (Wright et al., 2001). Moreover, there are cases, which require immediate revocation, and where using short validity certificates might lead to undesirable effects.

As an example where having short validity periods cannot be used as substitute for revocation, consider a distributed database containing data regarding various commercial companies. Assume that access to this database is subject to the well-known *Chinese Wall* policy (Brewer and Nash, 1989). Under this policy, companies are partitioned into a set of disjoint "competition groups", where each group contains companies that compete with each other in the market place. The Chinese Wall requires that once an agent gets information about a company in a group G, he should not be allowed to get information about any other company in G. If agent privileges are established by certificates with limited time periods, then a malicious agent may improperly gain access to data of several companies in a competition group G. This is because, during a certificate validity period, an agent may present the certificate to different servers of the database, maintaining data of various companies in G. Since the certificate is valid, several servers might authorize access.

This example shows that having short-lived certificates as substitute for revocation may not be appropriate. And we have argued that it may be