available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

PKI-based trust management in inter-domain scenarios

Gabriel López Millán, Manuel Gil Pérez, Gregorio Martínez Pérez, Antonio F. Gómez Skarmeta*

Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30.071 Murcia, Spain

ARTICLE INFO

Article history:
Received 18 March 2009
Received in revised form
8 July 2009
Accepted 6 August 2009

Keywords:
Trust management
Inter-domain PKI
Performance evaluation
PKI requirements
Cross-certification

ABSTRACT

Hierarchical cross-certification fits well within large organizations that want their root CA to have direct control over all subordinate CAs. However, both Peer-to-Peer and Bridge CA cross-certification models suits better than the hierarchical one with organizations where a certain level of flexibility is needed to form and revoke trust relationships with other organizations as changing policy or business needs dictate. It seems that this second approach better fits the current and next-generation inter-domain networking models existing in both the wired and wireless Internet. In this context, this paper analyses some relevant inter-domain scenarios and derives the main requirements in terms of cross-certification from them. It then describes the design and lab implementation of a pan-European scenario which is based on a research network composed by a set of organizations that may have their own PKIs running, and that are interested to link with others in terms of certification services. It provides a complete design, implementation and performance analysis for this complex scenario, including a procedure and practical recommendations for building and validating certification paths.

1. Introduction and motivation

Some Public Key Infrastructures (PKIs) (Kiran et al., 2002) are now starting to define and use certification structures based on advanced trust models (i.e. Peer-to-Peer and Bridge CA cross-certifications) rather than basic certification hierarchies. It is better serving the current Internet structure, which is defined as a set of interconnected networks acting as a single virtual network.

These certification models are based on the fact that each organization can manage its own PKI, and then to establish and revoke cross-links with others when necessary, for example, according to its internal policies or business needs. These links are based on cross-certification (Lloyd, 2001; Hesse and Lemire, 2002) processes, that is, procedures undertaken by Certification Authorities (CA) to define trust relationships. When two CAs are cross-certified, they agree to trust and rely upon the digital certificates issued by them. It allows easy and scalable trust management between certified entities.

Two main cross-certification models are being currently used: Hierarchical cross-certification, which defines trust relationships between CAs inside the same administrative domain, and Peer-to-Peer cross-certification, which defines trust relationships between two autonomous (either standalone or hierarchical) CAs. A third alternative is the Bridge CA (BCA) model, representing a trustworthy independent node, which establishes trust relationships with several non-related CAs. Every CA shares one (i.e. unidirectional relationship) or two (i.e. bidirectional relationship) cross-certificates with the BCA, thereby establishing a trust relationship between the CAs through this neutral point. A deeper analysis of those models can be found at Lloyd (2001).

* *Corresponding author*. Tel.: +34 868 887646; fax: +34 868 884151.
E-mail addresses: gabilm@um.es (G. López Millán), mgilperez@um.es (M. Gil Pérez), gregorio@um.es (G. Martínez Pérez), skarmeta@um.es (A.F. Gómez Skarmeta).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.08.004

In these three described cross-certification models, trust can be *initially* considered as *transitive*, that is, if A has a trust relationship with B and B with C, implies A has an *indirect* trust relationship with C. However, depending on the particular scenario and/or the involved organizations, this feature may or may not be desirable. Thus, before a cross-certificate is issued, all the requirements and constraints to deal with this issue (or similar ones) have to be negotiated and agreed between involved parties. Restrictions in cross-certification environments can be described using a well-known group of extensions, such as *Basic Constraints, Certificate Policies, Name and Policy Constraints* and *Policy Mapping* (Hesse and Lemire, 2002; Cooper et al., 2008). The main objective of these extensions is to differentiate between CA and end entities certificates, to specify certification policies under those certificates have been issued, and to establish restrictions in the certification path for new issued certificates.

According to this, the main questions arising are: which trust model (or combination of them) should be deployed in a real inter-domain communication network? What is the best option in terms of performance? How can an entity (end user, application or device) determine whether the certificate provided by any other entity from a different organization can be trusted or not? And how the user response time is affected by the number of intermediate CAs taking part of the inter-domain trust infrastructure?

As there is not a common and agreed answer for all these questions, just some basic recommendations from the industry and the standardization bodies, we think that the provision of a practical experience related to the definition of a large-scale inter-domain scenario can be of interest for PKI designers and implementers. It can also help to promote a wider adoption of cross-certification trust models. This is the main motivation of this paper, where we describe the design, implementation and performance measurement of a cross-certification scenario. For this, we have taken the requirements from several scenarios including a real pan-European research communication network built during the Euro6IX IST European research project (Euro6IX EU-IST Project Home Page), and which was composed by several security domains willing to link securely their certification services.

This paper is structured as follows. Section 2 describes the inter-domain scenarios that will be considered throughout this paper. The main requirements for these scenarios in term of PKI services, certificate extensions, and certification path building and validation are provided in Section 3. Later, Section 4 presents the design of a lab testbed, which is then used in Section 5 to validate the ideas presented in previous sections. Section 6 provides a discussion about the lessons learnt from our research work. Section 7 presents some related works. Finally, we conclude the paper with our remarks and some future directions derived from this research work.

2. Inter-domain scenarios

This section introduces three of the main current scenarios that demonstrate how the establishment of trust relationships between organizations may become a complex process.

2.1. *Identity federations*

This scenario is based on the definition of a trust relationship among service providers (*remotes organizations*) and identity providers (*homes organizations*), in order to allow the exchange of end user credentials and related information among organizations. Examples of identity federations are InCommon (The InCommon federation) or SWITCH (The SWITCH federation), for web services, and eduroam (Wierenga et al., 2006) for network services.

Although in federations composed by few participants it is not necessary to deploy a complex cross-certification system, there are others scenarios where the number of participant organizations makes difficult the management of single CA hierarchies. One clear example of this situation is eduroam, where more than 100 organizations, from 33 countries of three continents make use of the same network access service.

Identity federations like eduroam are already in production, giving network access service to thousands of users. Now, next steps head to the definition of collaboration among those federations; what is called *confederation*. For example, U.S. research and education community is working on a similar solution to eduroam for U.S. institutions (Internet2 Salsa-FWNA). It seems clear that these federations will end up establishing trust relationships to define a confederation. For example, a typical cross-certification scenario between a European PKI hierarchy and its USA counterpart could involve until six subordinate and root CAs between two belonging organizations.

2.2. *e-business BCA*

Nowadays, most of the e-business scenarios are focused on the establishment of trust relationships among companies and organizations around the world. We can find several organizations establishing trust relationships based on the Bridge CA model, in order to define common and neutral trusted entities. Some examples are the following:

- European Bridge-CA (EB-CA) enables a secure communication channel between businesses and public authorities, including 35 members among the main banks, assurance, and telecommunication companies around Europe.
- Chinese Taipei BCA allows interoperability among public and privates CAs, and defines a framework to enable certification services by bridging public root CAs, financial CAs and foreign CAs. This organization has issued more than 1.500.000 certificates, supporting more than 350 PKI services. It also supports four subordinates CAs and eleven CA companies.
- The last example is the Federal Bridge Certification Authority (FBCA), which enables transitive trust among U.S. entities cross-certified with the FBCA. More than 20 organizations (CAs) are collaborating under the FBCA umbrella.

2.3. *Telcos and service providers*

Another important scenario where the establishment of complex trust relationships is becoming an important matter for security administrators is the one composed by network