An Interdomain PKI Model Based on Trust Lists

Helena Rifà-Pous and Jordi Herrera-Joancomartí

Universitat Oberta de Catalunya, Rbla del Poblenou, 156
08018 Barcelona, Spain
{hrifa,jherreraj}@uoc.edu

Abstract. The penetration of PKI technology in the market is moving slowly due to interoperability concerns. Main causes are not technical but political and social since there is no trust development model that appropriately deals with multidomain PKIs. We propose a new architecture that on one hand considers that trust is not an homogeneous property but tied to a particular relation, and on the other hand, trust management must be performed through specialized entities that can evaluate its risks and threads. The model is based on trust certificate lists that allows users to hold a personalized trust view without having to get involved in technical details. The model dynamically adapts to the context changes thanks to a new certificate extension, we have called TrustProviderLink (TPL).

Keywords: trust lists, reliability in PKI, interoperability, certificate extension.

1 Introduction

PKI technology has been widely accepted as the best solution to provide secure electronic transactions through an insecure channel. However, its global market penetration to common applications of general use it is not yet a fact.

The key reason for the slow adoption of PKI solutions in mass media products [1,2] is due to interoperability concerns. Interoperability can not be simply characterized as a technology-only issue. In fact, it encompasses a wide range of technical, legal and political issues.

The PKI industry has addressed technical interoperability problems through a standardization process of data types and protocols. Nowadays, despite the flexibility of the specifications, PKI technology has achieved maturity and the basic interoperability goals between different vendor solutions are guaranteed.

Therefore, today's major drawback for the PKI adoption is the difficulty to deploy a cross-border solution due to differences in the countries legal and political framework. Governments are reluctant to recognize other nation's CAs if they do not take part in the quality control and, on the other hand, the scope of liabilities of a CA is not clear if the jurisdiction does not regulate it by law. Several proposals have been presented to overcome these problems such as cross-certification and Bridge Certification Authority. Yet, none of them has succeed

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 49–64, 2007.

because of the complexities involved in the management of such infrastructures and the generalist perspective in which they are based.

The contribution of this paper is defining a procedure to facilitate the integration and interoperability of different PKI islands. The aim is being able to deal with elements of external security domains without creating a unique and monolithic infrastructure that is unable to adapt to any change. Users are the last responsible entities of the trust assignment within their context. Facilities are provided to identify the scope and attributions of each authority so that end entities can easily take the more appropriate decision for themselves.

The rest of the paper is structured as follows. In Section 2, the main trust models and their challenges are reviewed. Section 3 presents the proposed architecture and describes the entities and elements involved. In Section 4 we specify the functionality of the proposed architecture. Finally, section 5 concludes the paper and outlines some ideas for future research.

2 Trust Models and Challenges

PKI is intended to establish and maintain trusted relationships. In order to reach such objectives, mechanisms to propagate trust from credited organisms to unknown entities have to be built. See in [3] a survey on interoperability issues of multi-domain PKI. Next, we review the main trust model proposals and we identify their most relevant challenges.

2.1 Trust Models

Single CA
PKI trust development has been studied and analyzed from PKI origins. The most simple topology architecture is the single Certification Authority (CA) model, that is, all certificates are issued by a unique CA. Although simple, this design neither scales well nor adapts to the society patterns, so it leads to the appearance of multiple interconnected CAs which manage communities of users that can not interoperate ones with the others.

Hierarchical PKI
The first attempt to solve the problem of having multiple interconnected trust islands was the hierarchical PKI structure that is managed by a Root Certification Authority (RCA). Trust is established in a tree-like fashion and flows from top to bottom. The RCA public key is the fundamental point of trust, or trust anchor, for evaluating certificate acceptability. In this model the path construction procedure is very simple, as a single path exists from any end entity up to the RCA.

However, deploying a global unique RCA is inappropriate for political reasons. There is not a consensus about whom it would manage the RCA and how it would do it. Thus the conclusion is that this model is only directly applicable within one domain, which is generally supported in one or several communities