A New Proposal at the ITU for X.509?

By Richard L. FIELD

Law Office of Richard Field
USA

Prepared for Asia PKI Consortium conference:

“The Common Denominators – Collaboration of Cross-Region on E-Government Application, Cloud Computing and Security”

13 June 2013
Sukosol Hotel
Bangkok, Thailand

Summary

This paper provides a brief introduction to a new proposal introduced at the ITU to re-define the X.509 trust model for e-signatures in the open environment. It also notes some of the other current activity in X.509 policy development.

Problem

A fundamental problem exists with the existing X.509 trust model for electronic signatures. Specifically, it is difficult, in an "open" PKI environment, for a relying party to easily discern the level of assurance provided by the certification authority (CA) when authenticating a certificate holder, due to variable factors such as certificate legal disclaimers, CA technical strengths and weaknesses, and other operational factors.

Under the existing X.509 trust model, three core entities are specified: the certification authority (CA), the certificate holder, and the relying party. The relying party relies on the CA for validity and accuracy of the certificate, which attests to the certificate holder's identity and/or authority to act in a specific situation or range of situations.

The existing X.509 trust model functions best in a "closed" model, in which all parties have existing relationships and can agree on allocation of risks, among other things. In an "open" environment, however, there is no pre-existing contractual relationship between the CA and a relying party. For electronic signatures, the potential exists for unexpected and unlimited use of the e-signature. Part of the CA's role is to authenticate the identity of the certificate holder. Authentication and its associated infrastructure can be done at any level of assurance, but greater assurance will entail higher costs. Since the market will bear only a limited fee structure for CA services, and since fraud against CAs cannot be fully prevented, CAs have universally opted to limit their direct as well as contingent costs, through operational means as well as through legal disclaimers.

These various CA cost and risk reduction techniques have created particular problems in cross-border recognition of e-signatures using CA-based PKI techniques. It can be problematic, as a matter of national policy, for a country to accept the risk that comes with a foreign e-signature in the absence of a remedy against the counterparty, the interloper, or the CA in the event of third party interloper fraud. Cross-border interoperability of e-signatures remains a significant barrier to international trade.

Proposal

A proposal addressing this problem has been submitted to the International Telecommunications Union (ITU) Telecommunication Standardization Sector, Study Group 17, to amend ITU-T X.509. The proposal, authored by David Chadwick, et al, and submitted April 2013, is entitled **"Adding the Role of technical and juridical expert to the X.509 trust model"**. A copy of the summary proposal is attached.

The proposal recommends that regulation of PKIs should be performed at three different levels: juridical, organizational, and technical. The many legal issues, in particular, can cause uncertainty internationally due to different country legal regimes. These issues include the validity of e-signatures, the validity of electronic contracts, the legal responsibilities of CA, certificate holders and relying parties, and privacy rules.

At the organizational level, policies range from self-regulation of CAs, to limited government intervention (such as voluntary accreditation systems), to complete control by governments.

At the technical level, standards developing organizations vary among countries, based on their political, economic and legal structures.

The proposal seeks to define this as a trust management problem. The task of establishing trust in a certificate thus involves grappling with the associated organizational, technical and legal issues. The proposal recommends the explicit addition to the X.509 trust model of an expert trusted third party, who can evaluate objectively the CA and its certificates and send recommendations to relying parties that will enable them to make informed decisions about relying on the certificates. The expert will have to be familiar with all relevant legal, technical, and operational issues. In order to accommodate the expert trusted third party, the proposal recommends changing the X.509 trust model from a three-party to a four-party one.

Status of proposal and implications

While it is acknowledged that the proposal addresses a valid issue in the open X.509 trust model, it is far less certain that it will progress or be approved in the form proposed. The proposal is currently in early study mode, and is not the basis for any international standard or industry requirement.

An obvious difficulty with the proposed four-party trust model is that the expert trusted third party will itself need to set conditions for its work and to limit its own liability (it is a common practice for law firms, for example, to provide legal opinion letters only with strict limitations on scope and liability). There is no obvious reason why a four-party trust model will not need to become a five-party model, and so on.

ITU and X.509 background

The X.509 trust model was developed in the early 1990's by the ITU. For a number of years, a large and robust community remained interested in standards for open systems interconnection (OSI) protocols, which divided the architecture into seven layers.

In recent years, however, the OSI marketplace has not been widely established. ITU activity in this area has dwindled markedly, as has participation in Study Group 17. Although contributions are usually made by country participants, in this case the study group leadership itself has introduced the proposal.

Study Group 17 will next meet at the end of August 2013, then again in January 2014. There may or may not be additional submissions on this matter.

In order for the proposal to be approved at the ITU level, it must generally go through the traditional approval process (TAP), which requires plenary approval (essentially unanimity by all 193 member states, though only a small handful usually vote). This means that any one nation can effectively veto a proposal.

A less commonly used alternative for approval could involve the Standards Assembly, which meets only once every 4 years (the last one in November 2012), but requires only a majority vote for approval.

Today, the ITU focuses on three significant areas: managing radio spectrum, assisting developing countries, and telecommunications standards development.

Other activity

Much of the activity in X.509 has been taken up by the PKIX Committee of the Internet Engineering Task Force (IETF). The IETF cites the ITU specifications for X.509, but uses its own request for comment (RFC) process.

There has been significant international attention on the recently issued draft **Reference Certificate Policy** standards, issued by the Information Technology Laboratory at the U.S. National Institute of Standards and Technology (NIST). The purpose of the NIST document is to identify a baseline set of security controls and practices to support a secure issuance of certificates by publicly-trusted CAs. It addresses operational controls, technical security controls, and other business and legal matters. The draft **Reference Certificate Policy** is consistent with the **IETF PKIX Certificate Policy and Certification Practices Framework**.

The draft **Reference Certificate Policy**, Draft NISTIR 7924, dated April 2013, is available online at:

<http://csrc.nist.gov/publications/drafts/nistir-7924/draft_nistir_7924.pdf>.

The public comment period was from 11 April 2013 to 7 June 2013.

A goal of the NISTIR 7924 policy is to address certificates used to secure websites and to sign software. A large industry forum whose membership includes most all the key players (including the certificate vendors and operating system vendors) is the CA/Browser (CA/B) Forum. The CA/B Forum has been working on this problem for several years, and has also been compiling PKI laws. While the CA/B Forum has been focused, to date, primarily on SSL and code signing, it recognizes that, in the future, the issues may merge with those of e-signatures.

In Europe, much of the normative standards are developed within the European Telecommunication Standards Institute (ETSI), which has a subgroup that does PKI specifications. This group works closely with the CA/B Forum.

Richard L. FIELD <field@pipeline.com> advises internationally in technology, payment systems and global electronic commerce law. He has been a U.S. delegate to the UNCITRAL Working Group on Electronic Commerce, has assisted the ASEAN Secretariat on legal interoperability issues relating to its Single Windows project for customs processing, and the ITU on its HIPCAR project on electronic transactions implementation in the Caribbean region. He is editor-in-chief (incoming) of the American Bar Association's International Law News, and past chair of the ABA Section of Science & Technology Law and its Electronic Commerce Payment Committee.