Use of a Validation Authority to Provide Risk Management for the PKI Relying Party

Jon Ølnes[1] and Leif Buene[2]

[1] DNV Research, Veritasveien 1, N-1322 Høvik, Norway
[2] DNV Certification, Veritasveien 1, N-1322 Høvik, Norway
{jon.olnes, leif.buene}@dnv.com

Abstract. Interoperability between PKIs (Public Key Infrastructure) is a major issue in several electronic commerce scenarios. A Relying Party (RP), in particular in an international setting, should not unduly put restrictions on selection of Certificate Authorities (CA) by its counterparts. Rather, the RP should be able to accept certificates issued by any relevant CA. Such acceptance implies not only the ability to validate certificates, but also an assessment of the risk related to acceptance of a certificate for the purpose at hand. We analyse common PKI trust models with respect to risk management, and argue that an independent, trusted Validation Authority (VA) may be a better approach for this task. A VA as suggested by this paper will also remove the need for complicated certificate path processing.

1 Introduction

Public key cryptography used with a PKI (Public Key Infrastructure) carries the promise of authentication, electronic signatures and encryption based on sharing of only non-secret information (public keys, names and other information in certificates[1]). The same information (the certificate) may be shared with all counterparts, to replace separate, shared secrets.

The counterpart (RP for Relying Party – relying on certificates) must be able to validate the certificate (with respect to validity period, revocation status, authenticity, and integrity) and interpret its content. In addition, the RP must decide if the quality of the certificate is sufficient for the purpose at hand, and whether or not to accept the issuer of the certificate (the CA – Certification Authority). The latter decisions should be based on evaluation of the risk to the RP.

While the quality of a certificate (chiefly determined by the CA's certificate policy) in most cases is the primary risk element, other aspects of the CA itself, such as

[1] Another term is "electronic ID". A PKI-based electronic ID usually consists of two or three certificates and corresponding key pairs, separating out the encryption (key negotiation) function and possibly also the electronic signature (non-repudiation) function to separate key pairs/certificates. To a user, this separation is normally not visible. This paper uses the term "certificate", to be interpreted as covering the electronic ID term where appropriate.

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 1 – 15, 2006.

nationality, financial status, and reputation may be important. Note also that the policy represents a claimed quality level, and assessment of compliance may be important. An RP will typically also be very interested in the liability taken on by the CA in case of errors, and the possibility for claiming liability if needed.

It is clear that, in particular in an international setting, an RP may need to accept certificates from a large number of CAs. Present approaches to interoperability are trust lists (trusted CAs and their public keys) and formation of trust structures (hierarchy, cross-certification, and bridge-CA) among CAs. We argue that all these approaches have shortcomings with respect to aiding the RP's risk management decisions. Trust structures imply the need to discover and validate potentially complex trust paths through the structures, a major concern in present PKI implementations.

This paper recommends a different approach, where interoperability is offered by means of a trusted Validation Authority (VA), serving as an independent trust anchor for the RP. The VA serves as a clearinghouse between CAs and RPs, and by trusting the VA the RP is able to trust all CAs that the VA answers for.

The model is based on policies and explicit, signed agreements. An overall validation policy for the VA's services is defined, and additionally RPs may define individual policies to tailor services to their needs. The RP has one agreement with the VA, and the VA on the other hand has agreements with the CAs, preferably in a model where one VA-CA agreement covers all RPs that the VA handles. Thus, all actors (including the CAs) obtain a clear risk picture. The VA handles all CAs individually, and as an added value the need for cumbersome certificate path discovery and validation procedures is removed. The RP obtains a one-stop shopping service for acceptance of certificates – one point of trust, one agreement, one bill, one liable actor.

In this trust model, it is important that the VA is neutral with respect to CAs, i.e. the VA service should be offered by an independent actor. In particular, this applies to judgments about quality and other aspects of CAs and their services.

In the following, we clarify DNV's position in 2, describe requirements in 3, take a critical look at existing approaches in 4, describe the independent VA in 5, present elements for certificate validation policies in 6, and conclude in 7.

2 DNV's Position and Role

DNV (Det Norske Veritas, http://www.dnv.com) is an independent foundation offering classification and certification services from offices in more than 100 countries. The maritime sector and the oil and gas industry are the main markets. DNV is also among the world's leading certification bodies for management systems (ISO 9000, ISO 14000, BS 7799 and others), delivering services to all market sectors.

DNV seeks to extend its existing position as a supplier of trusted third party services to digital communication and service provisioning. The first version of a VA service along the lines described in this paper will be offered to pilot customers 3Q 2006. This paper does not describe this pilot service but rather the research leading to the decision to launch the pilot service.