Trust Services for the PKI Relying Party – Interoperability with Risk Management

Jon Ølnes, Leif Buene, Trond Øverland, DNV AS, Norway
jon.olnes@dnv.com, leif.buene@dnv.com, trond.overland@dnv.com

1. Introduction

Interoperability for electronic ID (i.e. PKI-based cryptographic certificates) and e-signatures is a major issue in several electronic commerce scenarios. From the viewpoints of the actors, the ultimate interoperability requirements can be stated as:

- As an eID owner (certificate holder), I should be able to use my eID towards any counterpart, even in an international market.
- As an eID receiver (relying party, RP), I should be able to accept eIDs from all counterparts, regardless of the PKI used for issuing the counterpart's eID.

The eID owner is in control of her own situation. She enters an agreement with a CA (Certificate Authority) that can offer an eID service with the desired quality at acceptable conditions. The position of the RP is considerably more complicated. The RP cannot control its counterparts' selection of eID issuer, and placing restrictions on the counterpart's selection breaks the interoperability requirements stated above.

This asymmetry in the positions of the eID owner role and the RP role in our view illustrates that it is the RP's position that needs to be facilitated in order for PKI interoperability to be a reality. The eID owner has one trusted party to rely on: the CA. In this paper we propose that the RP also should need to rely on only one trusted party, termed a Validation Authority (VA). The basic idea is that when the RP receives an eID, no matter the CA, the eID is sent to the VA. The VA returns an answer on validity and possibly also other characteristics of the eID and the CA, such as quality parameters.

By introducing the VA as an independent trust anchor for the RP, we obtain the following:

- By trusting the VA, the RP is able to trust all CAs that the VA can answer for.
- The RP obtains one-stop shopping for eID validation – one contract, one liable actor, one point of billing, one software integration.
- The VA's services can be extended to risk management services, such as indication and possibly also assessment of quality of eIDs.
- The trust model for the RP is changed, and consequently the need for complicated path discovery and path validation procedures is removed.

The VA's services may be extended beyond eID validation, e.g. to provide verification of signed documents and other notary-related services. DNV is in the process of implementing such VA services, which will be launched in an international market.

2. eID Validation and Risk Management

In order to accept an eID, the RP must of course be able to validate the eID (check integrity and authenticity by means of the CA's signature on the eID, and determine that the eID is within its validity period and is not revoked) and to interpret the contents of the eID.

If this basic validation is successful, the RP may still need further risk assessment before the eID is accepted: Verify that the quality of the eID is sufficient for the purpose at hand, assess the liability taken on by the CA in case of errors and the possibilities for claiming liability, and potentially also assess other characteristics of the CA such as nationality.

In general, risk management requires agreements, and an RP cannot be expected to enter agreements with more than a few CAs. The CA's certificate policy is intended to be an "implicit agreement" but relying on general terms published in certificate policies may be considered too risky, and besides the policy may be written in a foreign language and refer to foreign legislation.

3. A new trust model for the RP

The reason for the asymmetry in the positions of the eID owner and the RP is in our view the "PKI paradigm" that only a CA can serve as a trust anchor[1]. When an RP receives an eID issued by a CA that it does not a priori trust, the measure devised in present PKI practice is to navigate trust structures (hierarchies, bridge-CAs, mutual (peer-CA) cross-certification) among CAs from a CA that is directly trusted to the new CA. Certificate path processing may be very complex and resource consuming.

Given the risk management approach described in 2, trust structures only partly provide the RP with the necessary guidance. Trust structures make it possible for an RP to obtain a trusted copy of the CA's public key. A trust structure may also give an indication of quality, if policy mapping is used for cross-certification and hierarchies enforce a common quality for the member CAs. However, (claiming) liability still remains an issue between the RP and the individual CA.

While a CA (eID issuer) is the correct trust anchor for the eID owner, the RP needs a trust anchor for the RP's own problem: validation of eIDs. This paper proposes to handle risk management for the RP by an independent, trusted validation authority (VA). An agreements-based structure is suggested, where the RP will have one agreement with the VA for validation of "any" eID, regardless of the issuer, and the VA will in turn have agreements with "any" CA. Handling the validation and agreement complexity in one place, common for all RPs that are customers of the VA, is feasible. The VA acts as a clearinghouse for eIDs, providing answers about validity, quality, and other aspects for all CAs that the VA handles. For liability, the RP will claim liability towards the VA, who in turn must transfer the claim to the erroneous CA if possible (however, this is of no concern to the RP). The model is shown in Figure 1 with the RPs' present situation (excluding trust structures) on the left and the VA approach on the right hand side.

In this model, the VA is an independent trust anchor, and by trusting the VA, the RP can trust (with assessed risk) all CAs that the VA can answer for. The need for complicated certificate path processing disappears, since there is no need to link the VA's answer to a CA trust anchor. All CAs are handled independently by the VA, although path processing may aid the VA's internal operation. It is important that such a VA is independent from the CAs, as all CAs must be treated on equal terms.

To the CAs, such a VA should also be a desirable construct. A CA cannot have agreements with all possible RPs, and this complicates risk management for the CA. Using the legal situation in Europe as an example, the EU Directive on electronic signatures [4] in principle leaves a CA issuing qualified eIDs with an unlimited liability. A VA will provide agreements that help to control this liability situation and thus may enable risk management even for the CAs.

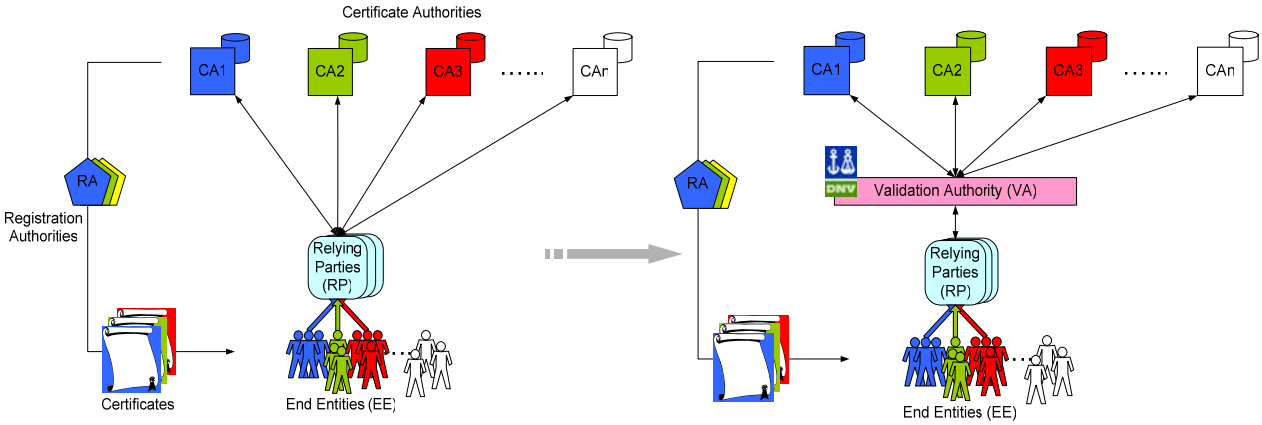

Figure 1: PKI interoperability without and with a validation authority.

4. Getting Rid of Path Processing

Certificate path processing is an issue that causes great concern in PKI deployment. We refer to [8] for a description of how complex certificate path discovery can be in general. Certificate path validation may be

[1] Trust list distribution services may be an exception to this rule, see end of 4.

very resource demanding due to the need for repeated certificate processing. Sufficient support for path processing is lacking in many PKI implementations. Certificate path validation, possibly also path discovery, may be performed by a validation service (delegated path validation/discovery [9]). The trust model suggested by this paper goes one step further by seeking to eliminate certificate path processing.

The mainstream approach to PKI interoperability today is bridge-CAs, which are being deployed with a regional scope (e.g. the US Federal Bridge CA – FBCA) or a defined business scope (e.g. the SAFE Bridge-CA [7] for the pharmaceutical industry). Indication of quality may be done by requiring a CA to cross-certify with the bridge-CA with policy mapping to the appropriate bridge-CA policy. E.g. the US Federal Bridge CA (FBCA) defines five policy levels [6]. However, bridge-CAs typically do not take on any liability and do not serve as trust anchors.

To expand interoperability beyond a bridge-CA's scope, bridge-CAs must be linked. The FBCA has defined guidelines for such cross-certification (part 3 of [5]). A preliminary conclusion of ongoing work [2] is that policy mapping must be dropped since policy frameworks for different bridge-CAs are too different. Thus, little is left of the risk management approach discussed in 2.

An approach that removes the need for trust structures and certificate path processing therefore seems like a good idea. Apart from a VA approach, such as suggested by this paper, a trust list distribution service may also eliminate certificate path processing. Lists of CAs and their public keys are regularly distributed, and interoperability is achieved by installation of compatible trust lists at all actors. In Europe, the IDABC Bridge/Gateway CA (EBGCA) actually is a trust list distribution service [3]. The primary purpose of the EBGCA is to list nationally approved or registered issuers of qualified certificates but other CAs may be added. The status of the CA (such as qualified certificates) is indicated as extra quality parameters of the trust list. Quality information is a fairly straightforward extension for any trust list.

The EBGCA is particular in that it defines itself as a trust anchor for the RP and takes on some liability with respect to the RP. In other cases, liability remains an issue between the RP and the individual CA. As for quality information, liability information may in principle be distributed with the trust list; however the distribution service is unlikely to help in claiming liability.

5. The VA's Services

Of the two alternatives that can eliminate certificate path processing, a VA approach may be preferred because a VA is able to provide a richer menu of value-added services to an RP. A suggestion for a "service stack" is shown in Figure 2:

- At the bottom lies validation of eIDs from "arbitrary" CAs.
- The classification service provides quality classification of eIDs and is strongly linked to eID validation. Classification may be provided either integral to eID validation (the validation reply provides the eID's quality) and/or as a separate service (may be viewed as a special case of auxiliary information).
- Signature validation allows third party verification of signed documents. The level of verification may depend on whether entire, signed documents are sent to the VA (requires strong trust in the VA since documents may need to be kept secret) or just (detached) signatures to be decrypted. Quality information may be provided, e.g. to indicate a qualified signature.
- Auxiliary information is derived from an eID. The service may be integral to eID validation and/or offered as a separate service. The typical example is name translation, where name(s) in the eID are translated into e.g. username (for a service), national identity number (where such exists) and so on. Other examples are age, sex, address and similar attributes. Auxiliary information may be general or customer specific and may only be given to customers that are entitled to use of the information.
- Trusted time stamping [1] is essential for electronic signatures. This service does not build on other services but may be a part of a VA's offering.
- Notary services are a natural extension of a signature validation service, providing trusted storage of signatures and verification traces, possibly also of entire documents. Maintenance of signatures (e.g. protection of old, weak signatures by a new level of signatures) and formats is necessary [10].
- The top level provides trusted repositories for data definitions (i.e. meta data for "the semantic web") and services to match an actor's requests with the offers of other actors based on a common set of data definitions. Reference data, as well as requests and offers, should be signed by the responsible actor. Services at this level are still mainly research topics and not ready for commercial exploitation.

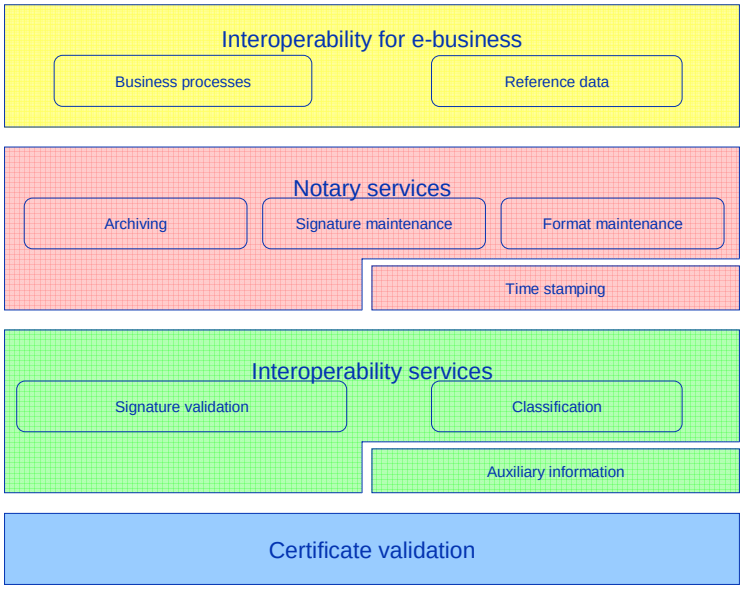

Figure 2: Interoperability services based on eID validation by a VA.

6. Conclusions

There is a need for a novel approach at trust services to assist the PKI RP role (Relying Party). This paper suggests use of a VA (Validation Authority), which can provide eID validation and possibly a set of further, value-added services to the RP. By introducing the VA as a separate trust anchor (which must be independent from the CAs), the RP is faced with one-stop shopping for eID validation: One contract partner, one liable actor, one software integration, one point of billing. As an additional, but important, effect, the need for complicated certificate path processing is removed.

References (only references used in this four pages abstract – more to be supplied)

1. Adams C., Cain P., Pinkas D., Zuccherato R.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol. RFC3161 (2001)
2. Alterman P., Blanchard D., Chokani S., Rea S.: Bridge-to-Bridge Interoperability. Panel presentation at the 5th Annual PKI R&D Workshop (2006)
3. Certipost: Certification Practices Statement, European IDABC Bridge/Gateway CA for Public Administrations v2.0. EBGCA-DEL-015 (2005)
4. EU: Community Framework for Electronic Signatures. Directive 1999/93/EC of the European Parliament and of the Council (1999)
5. Federal PKI Policy Authority (FPKIPA): US Government Public Key Infrastructure: Cross-Certification Criteria and Methodology Version 1.3. (2006)
6. Federal PKI Policy Authority (FPKIPA): X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) Version 2.1. (2006)
7. McBee F., Ingle M.: Meeting the Need for a Global Identity Management System in the Life Sciences Industry – White Paper. SAFE BioPharma Association. (2005)
8. OASIS: Understanding Certification Path Construction. White Paper from PKI Forum Technical Group (2002)
9. Pinkas D., Housley R.: Delegated Path Validation and Delegated Path Discovery Protocol Requirements. RFC3379 (2002)
10. J.Ølnes, A.Seip: On Long-Term Storage of Digitally Signed Documents. Second IFIP Conference on e-Commerce, e-Business, e-Government (I3E) (2002)