A DNSSEC-based Trust Infrastructure

Bud P. Bruegger, Eray Özmü

Fraunhofer IAO,
Universität Stuttgart
Nobelstr. 12,
Allmandring 35
70569 Stuttgart
bud.bruegger@iao.fraunhofer.de
eray.oezmue@iat.uni-stuttgart.de

Abstract: The management of trust issues is central to a wide variety of digital systems, including systems dealing with electronic signature, authentication, or signing of applications. The common approach to trust management is the use of possibly signed trust lists and trust stores that enumerate trusted issuers. This approach fails to scale well and is thus unsuited for the implementation of larger trust infrastructures, as, for example, in support of a regional authentication infrastructure that enables a marketplace of services.

This paper proposes to use the domain name system (DNS) with security extension (DNSSEC) as a base for the creation of a globally scalable and flexible trust infrastructure. As opposed to trust lists or stores, this also provides a vehicle for the efficient and secure dissemination of trust information among stakeholders.

1 Introduction

Trust decisions are crucial in identity and access management. While trust is an overloaded term, in this paper, it refers to the decision of whether a certain assertion can be accepted or whether it has to be rejected with an error message [Ca14].

Although being a central issue, the details of how to manage trust are often excluded from the scope of standards and systems. This is for example documented in [Ca14] for the case of the SAML 2.0 standard and the Shibboleth system. Instead, users of the technology are finally responsible for how they actually implement trust management.

The most common approaches to trust management are local trust stores and trust lists. Particularly for larger scale systems, they put a significant burden on relying parties who need to securely provision trust data (e.g., certificates or trust lists), keep them up to date, and query them for individual trust decisions.

To overcome these issues the authors present a trust infrastructure that is based on the Domain Name System (DNS) which scales very well, eases the burden on relying parties, and allows for highly efficient queries to support individual trust decisions.

While the proposed approach is applicable in many areas, for simplicity, the present description is limited to the use case of federated authentication. In particular, a relying party receives an assertion from some Identity Provider and needs to determine whether this assertion is trustworthy.

The STORK project [KO11] gives an example, how issuers of identities for authentication can be managed in various trust schemes (level 1 through 4) as determined by national trust scheme authorities.

The described trust infrastructure is part of the FutureID project [Ma13]. A minimal prototype has already been implemented.

The remainder of this paper is structured as follows. The next section describes previous and related work, also showing how the proposed approach solves problems experiences with the currently used trust lists. The main ideas of the approach are described in section 3. Section 4 draws conclusions.

2 Previous and related work

This section discusses the shortcomings of trust lists that are the most common current solution for large scale trust management. It then describes recent DNS-based technologies that have strongly influenced the proposed approach.

This paper focusses on a globally scalable trust infrastructure that supports an open number of trust schemes by arbitrary issuers. Relying parties make use of trust schemes to make individual trust decisions.

The most common solution for this problem are signed Trust Service Lists (TSLs) [ETSI09]. One of the best known examples is that of qualified certificates managed by the European Commission in support of legally binding signature [Ma13]. The Commissions TSL contains pointers that delegate the issuance of national TSLs to Member States who contain data of accredited issuers of qualified certificates. This single trust scheme is thus implemented by multiple TSLs.

Using TSLs, a relying party needs to locate and download the European and all national TSLs and keep them up to date. For individual trust decisions, it needs an efficient mechanism to query the data contained in the various TSLs.

Assuming that in a context such as that envisioned in FutureID, a relying party has to manage a significant number of trust schemes, relying parties also require a secure mechanism for locating the authentic TSLs of the various issuers.

The proposed approach eases the burden of relying parties as follows. Issuers of TSLs publish their data via DNS. Individual trust decisions can thus be based on a highly efficient single DNS query. Relying parties are relieved from managing updates. Also, the domain name is used to securely locate the desired trust data and thus largely facilitates the provisioning of trust anchors. DNS also provides native mechanisms for delegation.

The trust infrastructure proposed in this paper is an adaptation of DNS-based Authentication of Named Entities (DANE) [HS12] which uses DNS with its security extension to manage trust in TLS server certificates. Our approach thus joins a family of DANE adaptations in support of various trust problems, e.g., the association of OpenPGP public keys with email addresses [Wo13]. A master thesis [Jo00] illustrates how DNS queries are more efficient compared to LDAP queries for a similar problem.

3. A DNS-based trust infrastructure

This section gives an overview of how to use DNS to manage trust in assertions.

Figure 1 shows the three stakeholders and system components. Identity providers (IdPs) and relying party are well-known from federated identity managment. The trust scheme authority evaluated IdPs and publishes which IdPs have been found to be trustworthy. For this purpose, they operate a DNS server; relying parties use a DNS resolver.

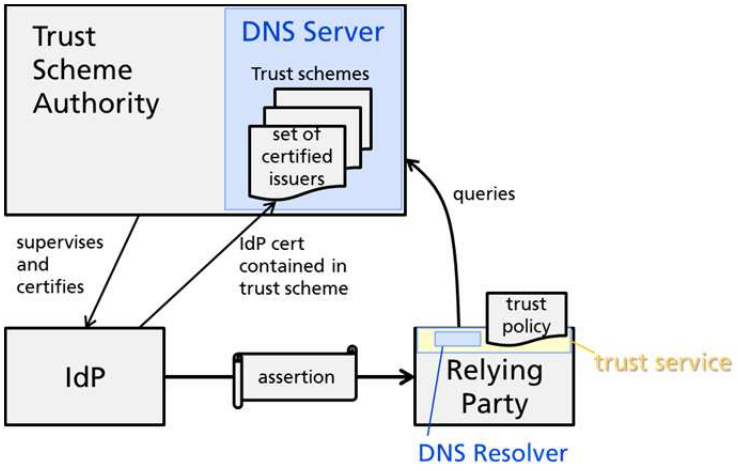

Figure 1 Overview DNS-based trust infrastructure for authentication

In the figure,a relying party receives an assertion from the identity provider. The relying party has to validate this assertion based on its issuer certificate and a trust policy.. The trust policy determines the trust schemes an acceptable IdP can belong to. Whether a

given IdP belongs to a given scheme is established via a DNS query where the scheme corresponds to a DNS domain and an issuer to a host. If the IdP is contained in the scheme, the query returns a digest of the issuer certificate.

3.1 Publication of sets of certificates by trust scheme authorities

This section describes how trust scheme authorities use the DNS to publish sets of IdP certificates. The use case is an Europe-wide certification of IdPs following the proposal by STORK.

A trust scheme authority is uniquely identified by its domain name. For example, the atrust scheme authority of the European Commission could use *tsa.ec.eu*. A trust scheme authority can manage several trust schemes. Each schema is represented by a sub-domain. For example, the European Commission may manage a scheme for authentication under *auth.tsa.ec.eu*.

Optionally, a trust scheme may be divided into several sub-schemes. For example, the STORK trust scheme distinguishes four assurance levels: *level1.auth.tsa.ec.eu* through *level4.auth.tsa.ec.eu*.

It is common that a trust scheme authority may delegate authority to geographic or other kinds of sub-authorities. Again, using common mechanisms provided by DNS, this can be expressed in terms of sub-domains: *at.level4.auth.tsa.ec.eu*, *uk.level4.auth.tsa.ec.eu*, etc.

Once all necessary schemes and sub-schemes are defined, the resulting sub-domains need to be populated with IdP certificates. To use DNS as dissemination vehicle, certificates thus need to be mapped to host labels.

Several options of how to map certificates to DNS host labels exist[1]. For the first prototypical implementation of the trust infrastructure only the base32-encoded digest of the certificate is considered. An example for a host label is *PX2NO4LVPA4WHCBLYXHIKRWVRE.at.level4.auth.tsa.ec.eu.*

3.2 Validation of electronic artifacts

A relying party who receives an electronic artifact must verify whether its certificate is permitted by the trust policy. The trust membership claim provided by the issuer helps to efficiently validate the artifact in two steps:

- Verify that the claimed membership satisfies the policy,
- Validate the claimed membership relative to a locally defined set or remotely with a trust scheme authority.

In the case where the set is defined by a trust scheme authority, DNS with DNSSEC extension offers all necessary mechanisms to securely validate membership. DNSSEC makes it possible to transfer data about set membership securely, in the sense that the relying party can verify that the information was provided by the trust scheme authority who controls the according domain name and that the data has not been tampered with in transit. DNSSEC further enables a trust scheme authority to assert the absence of a certificate from one of its sets.

With its delegation and caching mechanisms, DNS is proven to solve these kinds of queries in a globally scalable manner.

Relying parties require a high-level language to express which issuers of electronic artifacts they trust. A key element to reach a high level of expressiveness is to use named sets of certificates much rather than enumerating individual certificates. This provides a simple, but highly expressive language to express trust policy. An example for a trust policy could look like the following:

badGuys := [<PEM1>, <PEM2, .., <PEMn>]

employees:= [<PEM1>, <PEM2, .., <PEMm>]

trusted := (employees & level4.white.authentication.tsa.ec.eu) – badGuys

3.3 Trust Membership Claims by Issuers

In support of efficient verification of electronic artifacts, their issuer should use mechanisms to indicate to relying parties that they have been certified in a given trust scheme by some authority. We call this trust membership.

In the best case the trust scheme authority's sub-domain is already included in the certificate or the public key is directly listed in the assertion. Depending on the assertion this could be achieved in different ways. The fields Subject, or Issuer Alt Name in a certificate could be used give the respective information (e.g. *issuerAltName: PX2NO4LVPA4WHCBLYXHIKRWVRE.it.qualified-white.tsa.ec.eu*). In SAML assertions the same information could be inserted into one of the available fields. The trust membership claims could also be located on a specific domain of the issuer's webserver. This must be on a standardized location relative to the issuer's domain (e.g. www.someissuer.de/tsa-meta.txt).

The authors want to emphasize that the trust membership claims are not security critical and are not needed to be signed, since the trust membership claims are verified by the relying parties.

4 Conclusions

This paper has proposed a DNS-based approach for managing a globally scalable trust infrastructure. It operates the application domain that is currently covered by Trust Service Lists (TSLs) and adds a vehicle for efficient querying and validation of individual elements of such lists, thus avoiding the need to operate a local cache of data from a potentially large numbers of such lists and the complexity of keeping such a cache up to date. To facilitate large scale deployment, the proposed infrastructure makes use of the existing global name registration provided by the DNS and the existing DNSSEC trust anchors.

The proposed approach joins a growing number of initiatives, led by DANE, that apply DNS with security extension to trust-related application areas. It thus shares the objective of finding more secure alternatives to the traditional PKI-based management of trust. Thanks to the significant innovation of DANE, only a relatively small effort is necessary to extend its concepts to an interesting domain of application that is important for the large scale use of digital signature and large scale identity management infrastructures as those foreseen by the EC in support of an evolving single market of online services.

The proposed trust infrastructure has been conceived as part of the FutureID project that develops such an identity management infrastructure. It follows the same philosophy of decentralization used by the project. The proposed infrastructure will be implemented and demonstrated in this context.

References

[Ca14] S. Cantor, “TrustManagement,” Shibboleth, 25-Jan-2010. [Online]. Available: https://wiki.shibboleth.net/confluence/display/SHIB2/TrustManagement. [Accessed: 13-Jun-2014].

[ETSI09] “ETSI TS 102 231 V3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information.” ETSI, Dec-2009.

[HS12] P. Hoffman and J. Schlyter, “The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.” Internet Engineering Task Force (IETF), Aug-2012.

[Jo00] S. Josefsson, “Network Application Security Using The Domain Name System.” Jun-2000.

[KO11] Körting, Stephan and Diana Ombelli, “Mapping security services to authentication levels - Reflecting on STORK QAA levels.”. 2011 .

[Ma13] Martens, Tarvi, Keskel, Maili, Hühnlein, Detlef, Özmü, Eray, Ituarte, Nuria, and Rath, Christof, “WP43 - Trust Service.” FutureID, 11-Dec-2013.

[Wo13] P. Wouters, “Using DANE to Associate OpenPGP public keys with email addresses.” 21-Oct-2013.