A Service Oriented Trust Development Platform

Helena Rifà (Research Team Leader) - Dr. Francisco Jordán (CTO)

Safelayer Secure Communications, S.A.
{ hrifa | jordan }@safelayer.com

Abstract

A Trust Development Platform that offers services for the generation and interpretation of trust based on the concept of ecosystem's federation is presented. Trust federation schemes allow to define bonds of confidence between systems managed under different domains and policies. Each ecosystem has a trusted service provider that will automatically deliver services for the local domain following its own security policies. Ecosystem's federation leads us to the federation of trusted services providers and therefore, to the development of federated trust systems. Unlike solutions based on global trust policies, the proposed architecture is easy to deploy and use, and conforms to the requirements for each environment. Moreover, an ecosystem's federation is also feasible because a common language is shared, XML, and a plethora of related standards are based on it. SOA and Web Services are intimately related to federation, so trust development is now something almost tangible.

1 Introduction

The evolution of Information Technology's application environments has suffered many revolutions over the past decade. We are currently immerse in a revolution in which applications are replaced by services based on open architectures named Service Oriented Architectures (SOA) [MLB+06]. They are specially designed to overcome the integration and automation processes. Service access is standardized by a common language based on XML [YCB+04]. That allows abstracting the offered functionality from the implementation details thus providing a reference for the integration of different environments within an ecosystem (intra), and also among them (inter).

Security in terms of trust is vital when talking about the global integration and automation of information systems that are managed by different domains and under different policies. Trust development must initially refer to authentication and identification of the parties. The most robust and popular authentication and identification mechanism is currently based on PKI (Public Key Infrastructure) technology and uses certificates and digital signature.

PKI trust development has been studied and analyzed from PKI origins. The most comfortable and simple way to manage trust is by means of a hierarchic structure that is headed by a root authority. However, the conclusion is that all this is only directly suitable within a single security domain, which is generally used by one or several ecosystems, but always within one unique administrative domain. There has been multiple efforts to try and take trust development to inter-domain level. Examples are the proposal to implant a global root authority (inappropriate for political reasons), and the use of intermediate or bridge authorities (complicated for both technical and political reasons).

We present a Trust Development Platform (TDP) that offers services for the generation and interpretation of trust, based on the concept of ecosystem's federation. Trust federation schemes allow us to define bonds of confidence between systems managed under different domains and policies. Each ecosystem has a trusted service provider that will automatically deliver services for the local domain following its own security policies. Ecosystem's federation leads us to the federation of trusted service providers and therefore, to the development of federated trust systems. Unlike solutions based on global trust policies, the proposed architecture is easy to deploy, viable and conforms to the requirements of each environment. Moreover, an ecosystem's federation is also feasible because a common language is shared, XML, and a plethora of standards based on it. SOA and Web Services are intimately related to federation, so trust development is now something almost tangible.

The rest of this papers is organized as follows: In section 2 we overview the architecture of the TDP. Section 3 describes the concept of ecosystem's federation, pointing out the benefits of identity and trust federation. Section 4 explains the TDP security policies. In section 5 we review the most popular PKI trust models and describe how to overcome its weaknesses using the proposed TDP model. Finally, section 6 concludes the paper.

2 Trust Development Platform Architecture

Trust is a key issue to develop business, both in a traditional or in an electronic environment. In order to take direct decisions with a minimum risk, trust management creates a unified framework for specifying and interpreting security policies, credentials and relationships. In a closed virtual organization trust is commonly established with the use of Trusted Third Parties (TTP), and propagated in a hierarchical model. However, this architecture is not appropriate for a global scenario formed of isles of TTP: trust management can quickly become extremely complex and tedious for people to maintain. The solution is a TDP that automates the trust management to make decisions about trust as users (Relying Parties) themselves would do (see figure 1).

The key principles of a TDP are the following:

- Hiding trust development complexity producing a final diagnosis of the trust level of a transaction, operation, document, etc. Trust evaluation is performed from all the security data involved within an operation (certificate chains, certificate revocation lists, time stamps, …) considering the trust offered by TTPs (CA, VA, TSA..) that issued them.
- Delegating security configuration in a centralized system based on policies releasing the consumers (users, applications or other web services) from its complexity.
- Easing the use, integration and interoperability of digital signatures and envelopes, encapsulating all the standard formats (PKCS#7, CMS, S/MIME, XML-DSig, XAdES, XML-Enc, pdf, etc.) and its processing complexity under a common service interface.
- Providing a centralized point of accounting and auditing, and even trust archiving, thus making it feasible to manage and develop trust material for long periods of time.

On the other hand, it is important that a TDP can be easily integrated with other services and accessible from any device. Our proposal is to deploy a TDP as web services (WS), offering an interface fully based on Extensible Markup Language (XML). XML currently is the universal format to represent structured documents and data on the Web. In the TDP it is used in services invocations as well as in configuration, personalization, monitoring, audit and access control. TDP transactions are wrapped with SOAP, which defines a standard framework for the composition of request/response messages to a service. WSDL provides an abstract definition of the service independent of the programming language used in its implementation, and UDDI is used for the publication and discovery of the services.

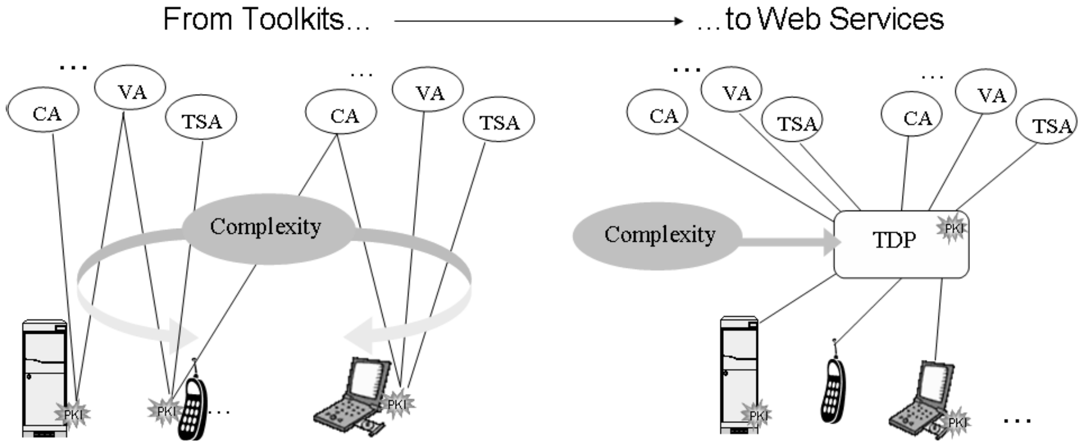

Figure 1: From Toolkits to Web Services

The proposed trust management framework is flexible and scalable and not only addressed to provide services for the internal security consumption. It can also be seen as a trusted platform that can be integrated in the enterprise workflows. The TDP provides business components with specialized trusted security services. The main TDP components are the following:

- An Authentication and Authorization service that includes different authentication mechanisms such as login/password, certificate-based (TLS/SSL, digital signature, etc.), etc.. This service also includes an open authentication extension mechanism (one-time password, tokens, kerberos, etc.) making possible the addition of new mechanisms. Access control is internally enforced and the Authorization service can be consumed through SAML protocol.
- An information management service which uses XML to provide uniform object and/or entity profiles: users, applications, web services, policies, certificates, logs/audit, etc.
- A digital signature service that allows to generate basic signatures in different well-known formats (PKCS#7/CMS, PDF, XMLDsig/XAdES and S/MIME).
- An advanced digital signature service that adds reliable time and revocation information to previously signed documents, as a base for long term signatures.
- A digital signature verification service (includes advanced or long term signatures) independent from the supplier, certificate verification mechanism (CRL, OCSP, etc.) and signature format.
- A digital signature custody service that enables to maintain the signature's validity for long periods of time by, therefore, implementing long term digital signatures by using XAdES ES-A standard.
- A document ciphering and deciphering service using PKCS#7/CMS and XML-Enc formats.

- A document ciphering key custody service that guarantees long term access to protected data.
- A key management service for key generation, registration, consultation, verification, etc., for instance, based on XKMS.

The access to the security services is performed with standardized WS protocols: Oasis DSS (Digital Signature Services), WSS (Integrity and confidentiality of SOAP messages) and SAML (Single-Sign On and Federation) are the basic standards.

Trust services are accessible for their composition, orchestration and consumption as any other business services from an SOA. The TDP facilitates to the rest of the business components a set of security specialized services that they can consume, such as:

- Authentication, authorization and unified access control
- Identity Federation
- Federation of attribute entity information
- Cryptographic key management, secure sessions, single sign-on, etc.
- Generation and validation of digital signatures
- Data protection
- Information notarization for non-repudiation using long-term digital signatures

3 Federation services

One of the outstanding characteristics of the proposed platform is that it offers federation services, both identity and trust federation.

3.1 Identity Federation

Identity federation can be defined as the agreements, standards and technologies that make identity and entitlements portable. Identity federation schemes allow decentralizing the user management thus distributing the identity data in partitioned repositories of different providers. They become a solution to increase sensible data protection and manage it uniformly in the most appropriate place.

In a federated environment, a user can log on through its identity provider and then use that authentication state to easily access resources in external domains. Since identity federation provides a mechanism to interchange sensible information regarding an individual to the service providers located in diverse security domains, users can ubiquily consume services catered to them without having to re-authenticate or re-establish their identity. Service providers can enforce access control using the applicant session token issued by federated providers and evaluating the security policies associated to the claimed identity.

Identity federation can help to enable Single Sign On (SSO), and provide users and customers with a more seamless and integrated experience. The benefits of successful federation projects include increasing security and control, cost reduction, simplification of the user experience and enabling the implementation of core business models.

But more importantly, identity federation enables the creation of a unique virtual identity that can be used to operate in any of the users services. That makes possible to achieve one of the principal goals of a TDP, the easiness of use.

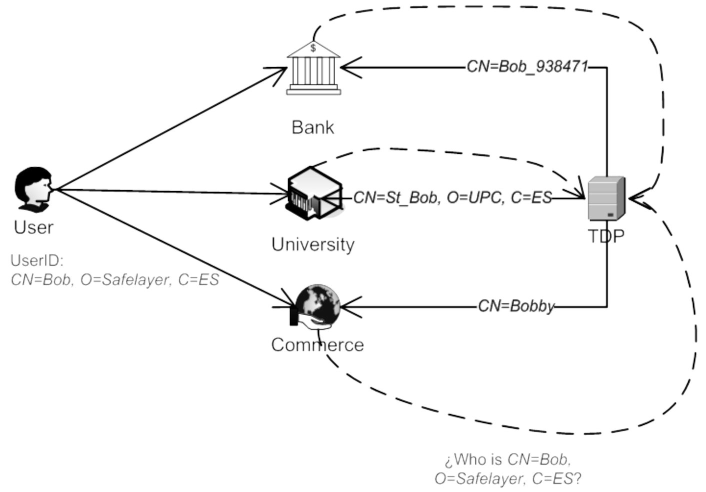

Figure 2: Identity Federation

3.2 Trust Federation

Trust federation allows defining trust bindings between different systems managed from different domains and policies. Nowadays, the most extended trust model is based on a public key infrastructure (PKI). Due to the lack of a global root certification authority (CA), the hierarchical model of the PKI has evolved into isolated and unconnected groups. Users that deal with security data generated in external domains have to manage by themselves a trust environment to handle these transactions, and this is complex and risky.

A federation scheme defines the trust rules between providers. These rules, expressed in XML, human readable and machine processable, allow to define with a great deal of granularity the trust placed in the security services offered by external providers. Therefore, for example, a TDP can accept the status result of a certificate whose chain is not registered in the system if it has a trust federation with another TDP that recognizes the named PKI and the security policies allow it.

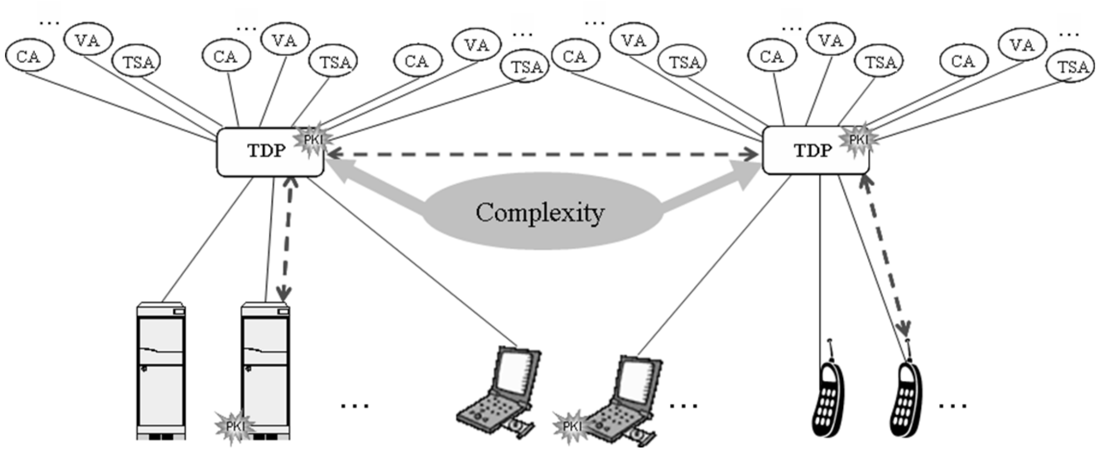

Figure 3: Federated trust management

A TDP offers security services that indicate the level of trust in the response information. The measure or trust classification is set considering all trust authorities involved in the process, i.e., Certification and Revocation Authorities (CA), Validation Authorities (VA), Time-Stamp Authorities (TSA), certification policies elements, etc. A TDP presents a clear and unique diagnosis result based on a centralized configuration (policy) that complies with some stipulated rules.

As well as Identity Federation, Trust Federation occurs in a bilateral way between Trusted Service Providers. Trust is developed more like Identity Federation in which a local name is mapped into another external name that becomes local for a remote provider. Thus, Trust Federation stands for the mapping of remote external security policies into local ones, by applying a set of rules defined in the local administrative domain.

One of the main contributions of a TDP is to uniform the trust domain management, that is, the enforcement of the system security policies.

4 Policies

The proposed TDP is a policy driven system. That means that the response of the system is based on a temporal context (running session) and the defined system policies. The establishment of policy based management solutions that cater for security has been impeded up to date because of the complexity to cope with heterogenous scenarios. It lacked some common language which could provide a unified approach to support the concepts of the policy models emerging from different research communities. Such a language has to fulfill the requirements of expressiveness, structure, composition, conflict resolution, extensibility and comprehensiveness, and XML does it. XML provides tools for designing textual descriptions of policies that are easy to generate and read by a computer, that are unambiguous, and that avoid common pitfalls, such as lack of support for internationalization/localization, and platform-dependency.

Security policies are the simplest solution to seamlessly deal with the growing complexity of secure and trust services. The TDP has tree types of security policies: authentication, authorization and service. The first two constitute the access control model. The service policies define the actions of the platform in front of a security service request, like the generation or verification of a digital signature. For example, in the case of a signature verification, the service policies would define the frame of trust with the external security providers, the security information details that have to be returned in a response, etc..

TDP manages the policies in a transactional cycle. When a service is requested, first of all, the authentication policy is applied. If successfully passed, an authorization policy is proposed and then evaluated upon the requested resource or service. If again passed, a service policy is proposed for the specific requested service. The latest policy is thus tailored for the service using information produced on the previous two phases. For instance, it is possible to restrict the algorithm of a digital signature generation service if the request comes from a particular IP address range, or during a time period (see figure 4).

Note that separating the management policy from the automated engines which interpret the policies facilitates the dynamic change of behaviour of a distributed TDP. This allows it to evolve adapting to system changes and new requirements. Changing the behaviour of the trusted platform can be achieved by changing the policy without having to re-implement nothing; this permits the use of the TDP in different environments.

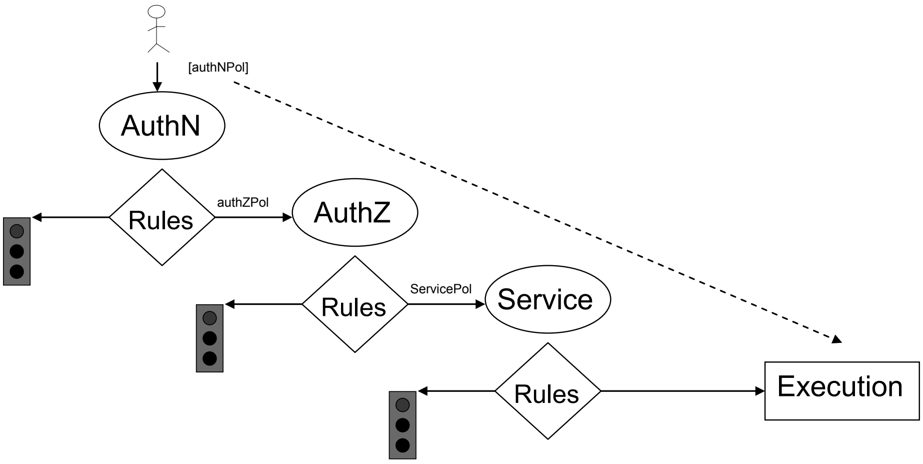

Figure 4: Dynamic Policy-based system

5 Trust Development Rationale

Our rationale for the proposed Trust Development model is a consequence of both i) several years of experience in PKI theory and real projects, and ii) the final conclusion that, everything that works on the Internet has been deployed in a bottom-up model, from a local to a wide domain, or deploy local and further interconnect with others.

Trust is a matter of locality and proximity. The furthest the party, the least it is trusted. This is the basic concept and the premise for our conclusion.

5.1 PKI Traditional Models

PKI trust development has been studied and analyzed from PKI origins. The most comfortable and simple way to manage trust is by means of a hierarchic structure that is managed by a root authority. Trust is established in a tree-like fashion and flows from top to bottom. In this model the path construction procedure is very simple, as a single path exists from any end entity up to the root CA. However, deploying a global unique root authority is inappropriate for political reasons. Thus the conclusion is that all this is only directly applicable within one domain, which is generally supported in one or several ecosystems generally forming different security domains, but always within one unique administrative domain.

There has been multiple efforts to try and take trust development to inter-domain levels. In the cross-certification model two CAs cross-certify each other if they agree to trust and rely on each other’s public key certificates and keys as if they had issued them themselves. The Certification Authorities exchange cross-certificates and enable users from one Certification Authority to interact electronically and securely with users from the other. However, the number of cross-certificates tends to grow exponentially, policy (semantic) mappings are very complex and it is difficult to build certification paths between two generic end entities. Although some vendors have implemented cross-certification in their PKI management products and the IETF has included CA cross-certification in its Certificate Management Protocol, cross-certification is still not well supported by common general-purpose applications.

The Bridge CA (BCA) trust model is similar to the cross-certification one. The BCA acts as a facilitator to interconnect other CAs. Each relying party just trusts its own CA which in turn trusts the bridge that finally trusts the remote CA, so that each member needs only to maintain a single cross-certification with the BCA and then it is automatically able to build certification paths across all spokes. Although this model is quite simple from the end user perspective, in fact it presents technical difficulties because the path construction is intrinsically complex and several checks (e.g. policy and name constraints, certificate status, policy mappings) must be performed throughout the certificate chain.

The Bridge VA (BVA) trust model is a further step to the Bridge CA. It solves more of the technical complexities, for instance, when dealing with path construction, and offers to the relying end entities a more comfortable service. The Bridge VA concept is near to the Trust Development Service Provider concept, but more limited in scope since the BVA model only takes care of certificate chain construction and validation.

5.2 The Problem of PKI: Technology or Model?

The European Commission concludes in its "Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures" [Comm06] (we quote the first paragraphs of the "3.3.2 Technological Challenges" clause to consider it fully endorses our view):

> *There is no simple answer to why the market for electronic signatures has not developed faster, but the market is facing a number of technical challenges. One frequently highlighted problem that could contribute to the slow take up of advanced or qualified electronic signatures in Europe is the complexity of the PKI technology. The often stressed advantage of PKI is that this technology uses the system of the "trusted third party" which allows parties that have never met to trust each other on the internet. In many of the current applications there seems, however, to be little interest from the service providers, essentially for liability reasons, to allow their customers to use their authentication device for other services. This is probably why the use of different one-time passwords (OTPs) is still dominating the market and there is little indication of this changing in the near future.*
>
> *Other factors could explain this slow take up: the lack of provisions in the Directive on criteria for electronic signature verification services to be provided by the CSP to the end user and, the lack of provisions regarding the mutual recognition between CSPs. Depending of the countries, there are various solutions to validate a certificate such as the Root CA, the Bridge CA and the Trust Status List. In the framework of cross-border eGovernment transactions, in the IDA II Programme, action on Bridge/Gateway Certification Authority has resulted in a Bridge/Gateway CA Pilot project which has identified not only technological problems but also legal and organisational ones.*
>
> *The lack of technical interoperability at national and at cross-border level causes another obstacle for the market acceptance of e-signatures. It has resulted in many "isolated" islands of e-signature applications, where certificates can only be used for one single application. EESSI has worked on common interoperability standards but most of the Member states have specified national standards in order to promote interoperability.*

On the other hand, there are the USA Government E-Authentication [GoAc06], and the FBCA (Federal Bridge CA) [GoFB06] initiatives. Nowadays, the FBCA is trying to interconnect with other Bridge CAs, but it is reporting both technical and operational problems (see Top 10 issues from [Blan06]). We believe that in essence, these problems are inherent to the model of trying to globally interconnect PKI islands from the top.

In the paper entitled "PKI Interoperability by an Independent, Trusted Validation Authority" [Olne06], most of the shortcomings of traditional PKI models are cleverly described. A Bridge VA model is presented, however, we believe this is just part of the whole problem we are facing of.

Clearly, we also support the idea that the PKI concept has a problem, however, we disagree that it is technical, but we definitively believe that the problem is on how the PKI is organized, i.e. it is on the model.

5.3 Trust Service Provider Model

As clearly shown from the overviewed models, PKI interoperability issues are more related to political than technical problems. Setting up a global uniform network of trust is not viable because trust is not transitive. Every domain must be able to manage its trust regarding other entities, defining how, when and why these external entities can interoperate with the domain processes.

For instance, let us stop at the first of the Top 10 Issues in the FBCA [Blan06], "Policy Mapping". Policy mapping following a bottom-up or local-to-wide strategy becomes very complicated since we are trying to map hundreds or thousands of local existing practices into a very few global common set of policies. Definitively, it is almost impossible to summarize everyone's local particular semantics into a single common view (the one from the BCA), when at the top level, we have loosed the precision and richness of the bottom local policy. However, it is very easy to accommodate or map a very high policy into the best local practice. It is just a matter of a local decision, just because trust is a local matter.

Our proposed model deals with independent administrative domains that may include a set of PKIs. Rules governing the interconnection of PKIs are defined in the TDP and are particular of each domain. Thus the trust model can be seen as autonomous and overlapped sets of PKIs. Users belonging to an administrative domain can manage data generated to/from other domains under the security policies stated in their local TDP. TDP is responsible for the management of trusted entities, creating the trust path construction and validation, talking various protocols (e.g. OCSP, LDAP, SCVP) etc. so that the end user does not need to know how to manage all produced data.

Because at the end, users and entities (applications, web services, etc.) do not deal with certificates, but with authentication tokens, documents and data that contains digital signatures and encrypted information, what a TDP must provide is an integral solution to develop Trust given any form of secured piece of information. Certificates, CRLs and CAs are only part of the whole picture. The TDP must also deal with other third party trusted information, such as certificate status tokens and VAs, timestamp tokens and TSAs, authentication and authorization tokens and AAs (Assertion or Attribute Authorities), etc.

A TDP system may be compared to a firewall. We can figure out a TDP device in corporate networks just providing Trust Development services to the corporate users and applications. Configuration of Trust Development is done locally, i.e., there exists a corporate policy that dictates in what exactly the "corporation" trust, and what are the needed external-to-local policy mappings to developed such a trust. In doing that, there is no need for close collaboration, participation or interference from external entities, it is a local corporate decission. Global technical standards, operational guidance and common practices are what local corporations need to help them to accurately implement their local trust policies. Whether a corporation trusts a couple of end-entity issuing CAs only to develop its business, or it trusts a BCA that embraces several CAs and millions of users, is a matter of the local policy. However, the TDP system must allow the corporation to establish a local policy that limits the scope of what a BCA establishes. In other words, not everything that a BCA tells to be trusted in some degree is trusted by the corporation in the same degree.

The conclusion is that like in other activities and communities on the Internet, the global activity takes place thanks to a web of interconnected local systems in which end users actually rely on to provide the services. Trust Development may be one of such services.

5.4 Semantic Trust

Another important feature of a Trust Development service provider is that it provides to its users truthful Semantic Trust. A TDP system behaves as a translator of complex trust expressed as a collection of data tokens in different formats (certificates, CRLs, OCSP responses, timestamps, assertions, etc.) that are issued by Trusted Third Parties into a simple trust diagnostic expressed in an easy and well known format. Relying parties (users, applications, business processes, etc.) can not easily know about the degree of trust they can deposit on a signed document or transaction. Instead, they rely on a TDP to develop trust and produce a clear diagnostic.

The TDP evaluates the local established rules upon the protected data. The rules define all constrains and mappings the local policy mandates for a given set of trusted third parties linked to a given kind of secure token (e.g. digital signature, etc.). The final diagnostic is given to the relying party in the form of a unique Trust Level.

The Trust Level is a number of four possible values, namely:

- 0: low level of trust,
- 1: medium level of trust,
- 2: high level of trust, and
- 3: very high level of trust.

The final Trust Level is calculated as the lowest Trust Level assigned to each Trusted Third Party that participates with some trusted token (certificate, crl, ocsp response, timestamp, assertion, etc.) in the evaluation of the protected data (.e.g. a digitally signed document).

The Trust Level is always accompanied of the local policy identifier that has been applied to reach the conclusion. This policy identifier is perfectly understandable by the relying party since it is locally defined. However, the evaluated policy rules could assert (map) that this is equivalent to some external policy which indeed came in the protected data. Providing the external policy identifier to the relying party is worthless since, basically, it does not understand it.

Optionally, the TDP can provide information to the relying party about all trusted material used in the evaluation. In this case, the Trust Level is provided for each trusted token, and optionally, accompanied with a Trust Label for better identifying the context or semantic of trust assigned to the TTP that issued them.

In this scenario, it is easy for a relying party to make a decision taken into account a Trust Level number, and if requested more detail, a local understandable policy identifier.

6 Conclusion

We presented a PKI model based on Service Oriented TDPs. The TDP is a new PKI component that acts as the trust anchor for relaying parties. The suggested appoach addresses PKI interoperability, quality of service, easy of use and seamless integration into business processes.

The pillars of the TDP scheme are identity federation, trust federation, and policy oriented architecture.

Identity federation allows joining the sparce electronic identities of a person from diverse infrastructuctures in a single robust virtual identity. This makes it possible for users to obtain ubiquity services destined to them without having to re-establish their identity and thus simplifying the user experience and increasing security and control.

Trust federation enables the interconnection of PKI islands. Independent third parties are federated in an administrative domain with a specific level of trust for each security service they offer. Users are released from having to gather and interpret the required information (usually unreachable to them) to evaluate the certificates, evidences or secured documents they manage. The TDP computes the trustworthiness of signed documents on their behalf and communicate the resultant report to them.

On the other hand, the TDP is a policy driven system which permits to highly adapt the responses of the platform to the actual context of the client. The system can dynamically change its behavior based on the ambient conditions that embrace the request and its data. Moreover, as policies are expressed in XML, the configuration of the system is portable and simple.

Finally, it is worth noticing that all TDP interfaces are based on an SOA and Web Services so it is very easy to integrate the PKI services in the business workflow since there are a lot of tools to automate the development and deploying work.

TrustedX [Safe04] is an implementation of the presented TDP. More information can be found at http://www.trustedwebservices.org.

References

[ACPZ01] Adams, C., Cain, P., Pinkas, D., Zuccherato, R.: Internet X.509 Public Key Infrastructure Time Stamp Protocols, IETF RFC-3161, August 2001.

[AdFa99] Adams, C., Farrell, S.: Internet X.509 Public Key Infrastructure Certificate Mangement Protocols, IETF RFC-2510. March 1999.

[Blan06] Blanchard, D. (Cybertrust): I-CIDM Bridge to Bridge Interoperations. 5th Annual PKI R&D Workshop "Making PKI Easy to Use". April 2006. http://middleware.internet2.edu/pki06/proceedings/blanchard-bridge-bbwg.ppt

[Comm06] Commission of the European Communities: Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures. In: Report from the Commission to the European Parliament and the Council. Brussels, March 15, 2006.

[FHM+06] Freeman, T., Housley, R., Malpani, A., Cooper, D., Polk, T.: Server-based Certificate Validation Protocol (SCVP). IETF RFC Internet Draft. June 2006.

[GoAc06] US Government: E-Authentication Secure Government Access. http://www.cio.gov/eauthentication/

[GoFB06] US Government: Federal Bridge Certification Authority (FBCA). http://www.cio.gov/fbca/

[HFPS99] Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF RFC-2459. January 1999.

[LMMP05] Lioy, A., Marian, M., Moltchanova, N., Pala, M.: PKI past, present and future. Springer-Verlang 2005.

[MAA+99] Myers,M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. IETF RFC-2560, June 1999.

[MLB+06] Matthew, C., Laskey, K., McCabe, F., Brown, P., Metz, R.: Reference Model for Service Oriented Architecture 1.0, OASIS Technical Committee Specification, July 2006.

[Olne06] Olnes, Jon (DNV Research): PKI Interoperability by an Independent, Trusted Validation Authority. In: Proceedings of 5th Annual PKI R&D Workshop "Making PKI Easy to Use". April 2006.

[Safe04] TrustedX White Paper. Safelayer Secure Communications S.A., 2004-2006. http://www.trustedwebservices.org

[YCB+04] Yergeau, F., Cowan, J., Bray, T., Paoli, J., Sperberg-McQueen, C.;., Maler, E.: Extensible Markup Language (XML) 1.1. W3C Recommendation, April 2004. http://www.w3.org/TR/2004/REC-xml11-20040204/

Keywords

Public Key Infrastructure, Service Oriented Architecture, Trust management, Federation, Single Sign On, Security Policies