Mingchao Ma, Christoph Meinel:
A Proposal for Trust Model: Independent Trust Intermediary Service (ITIS)
in Proceedings of the IADIS International Conference WWW/Internet 2002 (ICWI 2002), IADIS Press, Lisbon, Portugal,
pp. 785-790, 11, 2002. ISBN: 972-9027-53-6.

A PROPOSAL FOR TRUST MODEL:*

INDEPENDENT TRUST INTERMEDIARY SERVICE (ITIS)

Mingchao Ma
Institute of Telematic
Bahnhof Straße 30-32
D-54292, Trier
Germany
ma@ti.fhg.de

Christoph Meinel
Institute of Telematic
Bahnhof Straße 30-32
D-54292, Trier
Germany
Meinel@ti.fhg.de

ABSTRACT

Reliable, distributed applications based on Internet, such as e-commerce system rely heavily on trust path among involved parties. This article introduces an efficient trust model based trust service, Independent Trust Intermediary Service model using Smart Trust List, for trust management. Fundamentally, Independent Trust Intermediary Service is facilities for distributing certificates of CAs in a manner that ensures their authenticity and integrity.

KEYWORDS

Security, Trust Management, Certificate, Cross Certification, Smart Trust List.

1. INTRODUCTION

There are ever increasing needs for public-key systems to provide security in network protocols, particularly in electronic commerce. Public key cryptography allows parties who were previously unknown to each other to establish trust-relationships and possibly conduct secure and encrypted communications on open network (e.g. on Internet). *Public-Key Certificate (PKC)*-A data structure containing the public key of an end-entity and some information, which is digitally signed with the private key of the CA which issued it (Aresenault & Turner, 2000). Certificate may be chained to form a certificate path. A certificate path is a chain of certificates. Each certificate in the certificate path is singed by its predecessor's private key. A relying party verifies a signature by successively verifying the signatures on the certificates in the path. Relying party depends on chains of certificates in order to determine whether or not to accept a given key as representing a particular principal. The chains extend from "trust anchor" point, which verifiers directly accept as reliable, reaching certified principals through zero or more intermediary (Introducers or CAs).

One of the current bottlenecks is the construction of trust chain under certain control. For example, one user, says Alice, who wants to buy a computer online, visits the website, say “E-Shop”, which is an online shop that provides very good price for the consumers. The problem is Alice has no any ideas about this website. Although Alice can download the certificate of the website, it is very possible that she can not verify it because she can not form a “trust chain” extend from her “trust anchor”. Considering this dilemma

* In Proceedings of IADIS International Conference WWW/Internet 2002, Nov.2002,Lisbon, Portugal, pp.785-790

in B2C market, consumers cannot trust the online shop and there is no effective way to convey trust to consumers.

In order to satisfy such requirements, we propose a general framework to convey trust under certain control for trust management. Our system, Independent Trust Intermediary Service (ITIS) provides a simple effective method to construct a delegation trust chains from source of authority to the requester. At the same time, it is also easy to integrate other trust services (e.g. Credit service) into the system to provide additional services. This model is very suitable for B2C and solves the trust transitive problem. It can also be used as a trust management server in a large company.

In Section 2, we will review some existing models and point to the problems with them. Section 3 discusses our approach to trust management. Section 4 describes Smart Trust List in details. A detailed example is presented graphically in Section 5, and we draw a conclusion and future direction in Section 6 and 7.

2. CURRENT TRUST MODELS

Some trust models have emerged as public key technology have grown beyond local domains to satisfy needs of larger and more diverse communities, such as PGP trust web (Zimmermann, 1994), direct cross-certification (CA_CA Interoperability, 2001), bridge CAs (William & Nelson, 2000), browse trust list and so on. These systems are based on the notion of delegation, whereby one entity gives some of its authority to other entities. The two well-known certificate systems are those of PGP and PKIX (Public Key Infrastructure based on X.509).

PGP uses a convenient means of using trust, associating trust with public keys, and exploiting trust information. PGP employs a structure called key ring to implement an “introducer mechanism”. Each entry in the public-key ring is a public-key certificate. Associated with each such entry is a key legitimacy field that indicates the extent to which PGP will trust that this is a valid public key for this user; the higher the level of trust, the stronger is the binding of this user ID to this key. Also associated with the entry are zero or more signatures that the key ring owner has collected that sign this certificate (by introducer).

If user A has a copy of user B's public-key record in some way that ensures its authenticity and integrity, then A can sign this copy and pass it to user C. A thus acts as an introducer of B to C. As PGP has grown in popularity, a decentralized "web of trust" has emerged. In this type of system each user creates and signs certificates for the people he or she knows. Similarly, each individual must create his own key pair and disseminate his own public key. Therefore, no central infrastructure needs to be developed. This model works very well for small groups, who have pre-existing relationships, but it doesn't scale well for large groups or where consistency of assurance is important. Communication of certificate status to relying parties (such as a revoked certificate) is also very difficult with this model.

The PKIX authentication framework (Housley et al., 1999) attempts to solve the same part of the trust management problem that PGP's introducer mechanism attempts to solve, namely the need to find a suitably trustworthy copy of the public key of someone with whom one wants to communicate. However, PKIX differs sharply from PGP in its level of centralization of information. While anyone may sign public-key records and act as an introducer in PGP, the PKIX framework requires that everyone will obtain certificates from a certification authority (CA). Relying parties who share a common CA can trust each other directly. Certificates from different CAs can’t trust each other unless there is pre-trust relationship between the CAs. Obviously it is impossible to organize all CAs into a global “certifying authority tree” and to have keys signed by CAs with a common ancestor in this global tree. A most common PKIX implementation is that of the Browser Trust List model, where each user application has a list of the public keys for all the CAs that user trusts. This model, implemented in Netscape and Microsoft web browsers, allows each user a great deal of flexibility to add and remove CAs from the trust List. However, a malicious party could potentially append a bogus CA certificate into the list and from then on have their bogus user certificates validated by the browser. The primary concern with this model, however, is that user must manage all of details about certificates. Another problem is software merchants who hard-coded these certificates into browser will not take any potential responsibilities caused by misusing those hard-coded certificates.

Obviously, we need a mechanism to convey the trust from where is exits to where it is needed. Our approach is a trust service that provides trust information, which can be used by other consumers to make a

trust decision. We can deem it as the same as the other services that provided in the internet, such as email service, ISP service, search service and so on.

3. INDEPENDENT TRUST INTERMEDIARY SERVICE (ITIS)

Reliable, distributed applications based on Internet, such as e-commerce system rely heavily on trust path among involved parties, but the nature of Internet is distrust because the involved parties are invisible to each other. This dilemma can be solved by using a trusted intermediary (TI) (Ketchpel & Garcia-Molina, 1996), which is basically an agent trusted by and accountable for both involved parties.

Our approach, Independent Trust Intermediary Service, is inspired by browser trust list and trusted intermediary. One of the reason that browser trust list model is the most common trust model is its simplicity. On the other hand, trusted intermediary provides a flexible and scalable mechanism for trust management, especially suitable for Internet. Combination of simplicity of browser trust list and flexibility of TI satisfies the needs of trust management in a distributed environment. Fundamentally, ITIS is facilities for distributing certificates of CAs (root CAs or subordinate CAs) in a manner that ensures their authenticity and integrity. Multi-ITISs connect each other to form a trust web. Relying party who consumes the service of a selected ITIS can deem it as "trust anchor" to form a trust chain. In this way, relying parties offload the burden of trust management to the selected ITIS. Relying parties just need to maintain a few certificates of their selected ITISs. Once the ITIS network is in place, any PKI system that wants to enlarge the acceptable scope of certificates can publish its certificates of CAs and other necessary information to selected ITISs. ITIS will first evaluate the registration information to make a decision whether or not accept these certificates. It will assign a security level to each accepted certificate according to registrant's security policies. All these trust information formed trust records will be stored in Smart Trust List, which will be discussed in Section 4. In addition to PKI systems, other services provider such as credit service can also register their verified certificates. In this way, ITIS can provide other value-added services.

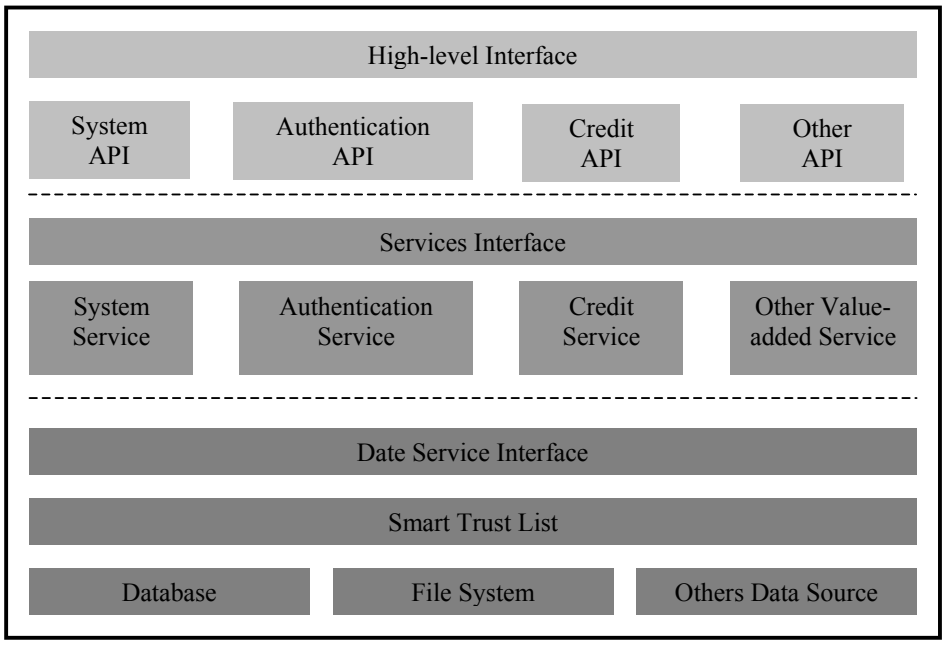
3.1 ITIS Architecture

The ITIS is designed for deployment as a trust service platform. Much like the network reference model, ITIS contains a series of layers which provide each level of abstraction, with higher layers building on the capabilities provided by the lower layers, shown in Figure 1. The High-level interface presents a series of system-independent APIs, which hides most of the implementation details, to external entities. The service layer contains a set of processing methods for the advertised services. It includes the business-aware rules and control functions. Note, as a trust service platform authentication service is the basic service. Any requirements from external entities must be authenticated firstly. The data layer stores the service-related data include certificates, security policies and other business policies for value-added services. This open architecture allows us to easily integrate new services into existing system by defining additional interfaces and creating the implementing service object and required data sources for the new services.

As a trust service provider, ITIS takes corresponding responsibilities for trust management, namely risk of decision is transformed. Relying parties who consume ITIS's service only maintains the public key of his or her trusting ITIS. Although it is possible for relying parties to trust multi-ITISs, the number of public keys maintained by users is much less than those in Browse Trust List. Relying parties is free to select ITIS by some means, such as a private favorable relationship, positive past experience or simply by reputation, rather than unqualifiedly accepting certificates hard-encoded by software merchants. Note that ITIS just imports the certificate of service provider instead of cross-certification, which is different from direct cross-certification technology. One of advantages is that ITIS can cancel any trust relationships by removing the record in Smart Trust List instead of maintaining a certificate revocation list, that means status of trust relationships is always "fresh". Another advantage is that ITIS can obtain Certificate Revocation List efficiently since service providers will register the methods of retrieval of CRL as well as their certificates. The propagation of revocation information is instantaneous.

3.2 ITIS Web Architecture

Each ITIS stores information about its trusted neighbors in its trust database. Multi-ITISs form a trust web. ITISs act as both servers and clients in the trust web. As servers, ITISs expose their services through their interfaces. Trusted client can consume the services by invoking these exposed interfaces. ITISs become clients when they invoke other ITISs' methods. The interface is a purely declarative component that hides the implementation details. This deliberate strategy facilitates interoperability and software integration.



ITIS Architecture
Figure 1

4. SMART TRUST LIST

Each ITIS maintains a Smart Trust List similar with browser trust list in the trust database shown in Table 1, but it is different from browser trust list as follow:

- Smart Trust List locates in Independent Trust Intermediary Service server instead of client's browser.
- Smart Trust List provides fine-grained trust level configuration to represent appropriate sets of authorities.
- Smart Trust List supports multi-kinds of certificate, e.g. X.509, XML Certificate
- Smart Trust List can support value-added services more than authentication services

Every certificate of CAs has a security level assigned by ITIS on registering. ITIS evaluates security policies of CAs and calculates security level according to a common set of security policies, which accepted by both ITIS and service providers. A common set of security policies is very important for security evaluation crossing domains. The Method of retrieval of CRL can be any online methods (e.g. OCSP (Myers et al., 1999)). By this way, ITIS can instantly acquire status of certificates. Service provider types maybe PKI service provider, credit service provider and so on. A description maybe includes any information about the service provider such as the name, location, owner of the service provider and so on.

Table 1 Smart Trust List

Certificate	**Certificates of CAs**
Security Level	**Assigned by the ITIS**
CRL retrieval	**How to retrieve CRL**
Description	**A comment about service provider**
Types	**Service provider types**

Every certificate of CAs has a security level assigned by ITIS on registering. ITIS evaluates security policies of CAs and calculates security level according to a common set of security policies, which accepted by both ITIS and service providers. A common set of security policies is very important for security evaluation crossing domains. The Method of retrieval of CRL can be any online methods (e.g. OCSP (Myers et al., 1999)) in such way that ITIS can instantly acquire status of certificates. Service provider types maybe PKI service provider, credit service provider and so on. A description maybe includes any information about the service provider such as the name, location, owner of the service provider and so on.

5. AN EXAMPLE

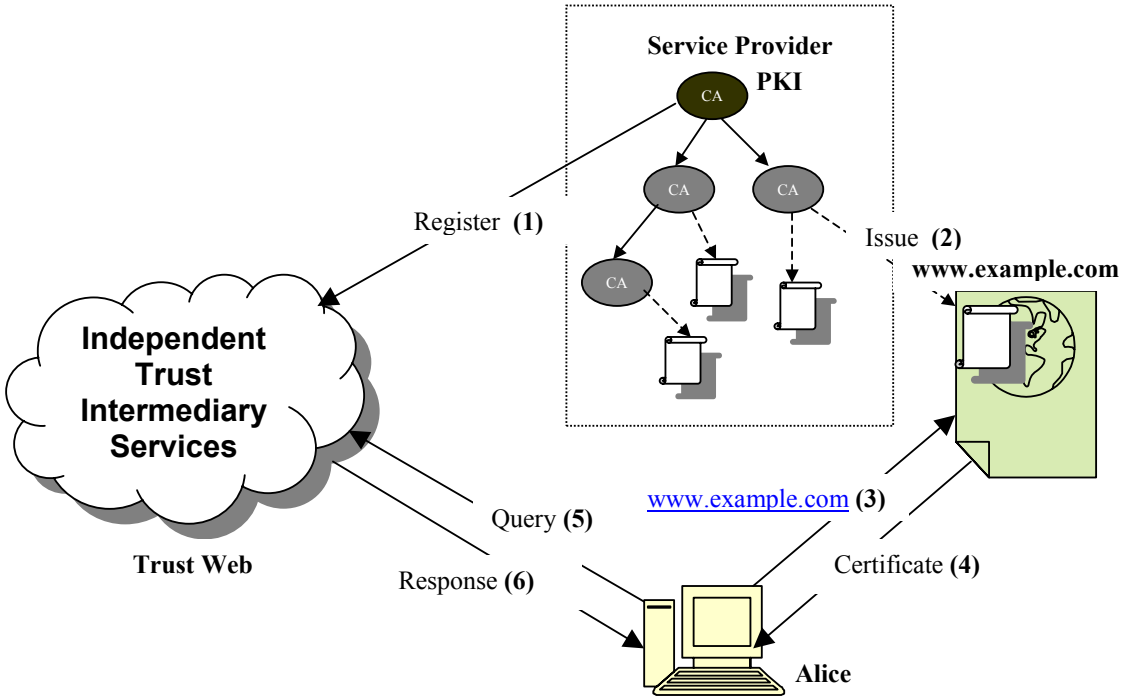


Figure 2

Figure 2 illustrates how the user might consume the trust service. Suppose four entities, a PKI system, a website, ITIS trust web and a client Alice, are interacting across a network. The PKI system publishes its certificate of root CA and optional subordinate CAs on the selected ITIS in a security way, possible offline way (1). ITIS will evaluate the PKI system's security policies and assigned a security level to it. A user, says Alice, will visit a website, says www.example.com, which has a certificate issued by a subordinate CA (2) to buy a computer. Alice points to the website (3) and downloads the certificate of the website (4). In order to verify the certificate, Alice sends a query message with the certificate to the selected ITIS. ITIS can verify the certificate because it has known the certificate of root CA. After that ITIS will response a message to inform the Alice the status of the website's certificate, security level and an optional brief description of the service provider. According to these message Alice can decide whether or not trust in the website and buy the computer from it.

6. CONCLUSION

We introduce our approach to trust management, Independent Trust Intermediary Service, which has followed features:

- Redistribution of risk in terms of risk management
- Simplicity of management in terms of technical challenges associated with large-scale systems
- Trust transitivity under certain control
- Flexibility and Scalability, provides basic authentication and additional trust services
- Logically centralized, physically distributed

Redistribution of risk by involving a trust third party is well-know concept in physical world. A good example is the bank; consumer and merchant can conduct a transaction with the help of a trust third party: bank, even though there is no pre-existing relationship between consumer and merchant. The trust third party facilities the public key distribution and management, thus it is easy for common users to form a "trust anchor" to verify the public key.

7. FURTHER WORKS

Automatic machine processing, including service registry, policy compare and analysis, trust negotiation and evaluation, needs a set of common standards, such as common security policies, business-policies and so on. This is the problem of establishing a common domain-special ontology policies agreement, which is particularly critical in our system. One solution achieves policies agreement through a scheme inspired by XML namespace. World Wide Web Consortium (W3C)'s RDF (Resource Description Framework, Lassila & Swick, 1999) and Web Ontology should be a good starting point.

REFERENCES

Bruce Schneier, 1996. *Applied Cryptography Protocols, Algorithm and Source Code in C, Second Edition.* John Wiley & Sons,Inc., New York.

William Stallings, 1998. *Cryptography and Network Security Principles and Practice, Second Edition.* Prentice Hall, Upper Saddle River, New Jersey.

Aresenault A. & Turner S., 2000, *Internet X.509 Public Key Infrastructure*, PKIX Working Group

CA_CA Interoperability, 2001, PKI forum's Technology Working Group (TWG), available at http://www.pkiforum.org/pdfs/ca-ca_interop.pdf

Housley et al., 1999, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile,* RFC2459, Network Working Group

Ketchpel S. P. & Garcia-Molina H., 1996, 'Making Trust Explicit in Distributed Commerce Transaction', pp.270-281, *Proceedings 16th Int'l Conf. Distributed Computing Systems*, IEEE CS Press, Los Alamitos, Calif.

Myers et al., 1999, *PKIX Online Certificate Status Protocol (OCSP)*, RFC2560, Network Working Group

P. Zimmermann, 1994. *PGP User's Guide*, MIT Press, Cambridge, USA

Ora Lassila & Ralph R. Swick, 1999, *Resource Description Framework (RDF) Model and Syntax Specification*, W3C Recommendation, available at: http://www.w3.org/TR/REC-rdf-syntax/

William T. P. & Nelson E. H., September 2000, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of 'Standards and Technology, available at: http://csrc.nist.gov/pki/documents/B2B-article.doc