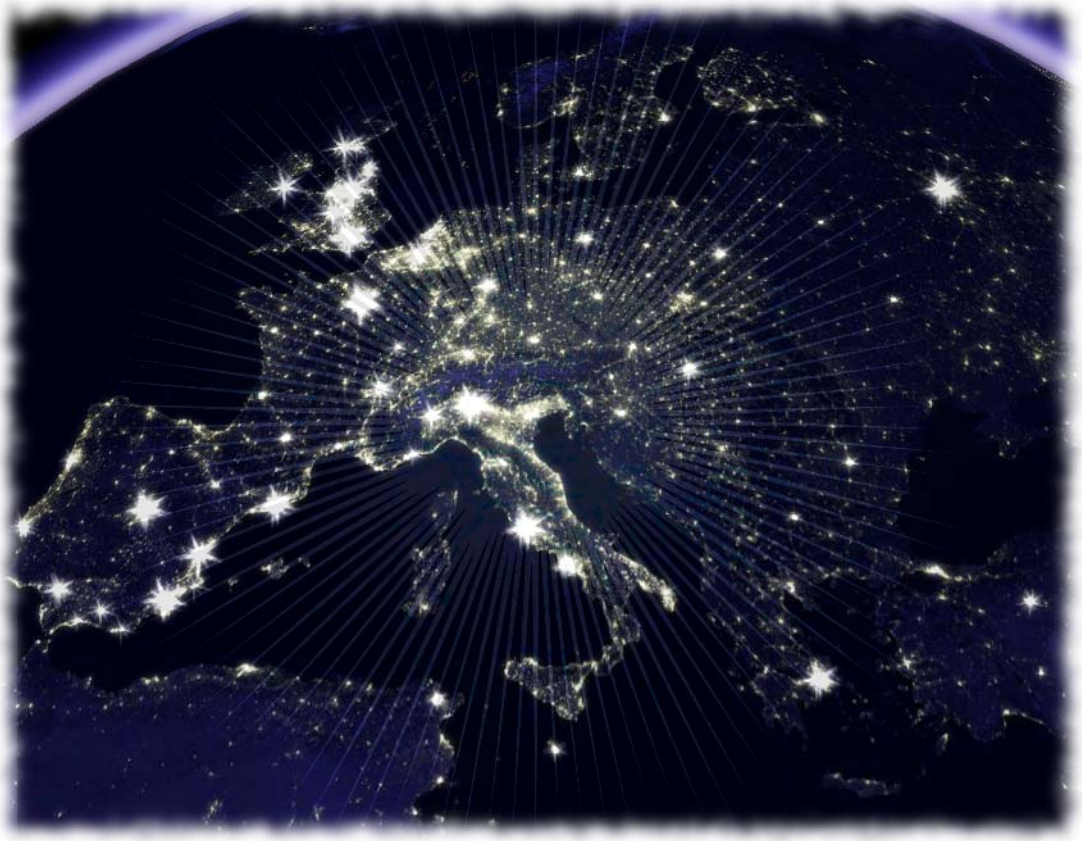
JRC Scientific and Technical Reports

Building Trust Networks

Petteri Ihalainen



EUR 23774 EN - 2009

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the JRC-IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies.

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: Via Enrico Fermi, 21027 Ispra (VA), Italy
E-mail: petteri.ihalainen@jrc.it
Tel.: +39 0332 78 3042
Fax: +39 0332 78 9567

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 50574

EUR 23774 EN
ISBN 978-92-79-11631-5
ISSN 1018-5593
DOI 10.2788/82918

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

Building Trust Networks

Introduction

The common agreement in the industry is that the Public Key Infrastructure is complex and expensive. From the year 1976 with the introduction of public key cryptography and the introduction of PKI concept in 1977 a lot of scientific resources has been spent on creation of usable key exchange systems and concepts to build trust networks.

Most EU Member States have implemented their own national Public Key Infrastructure solutions mainly to enable strong authentication of citizens. They are however not the only systems within the EU to utilize PKI. Due to the nature of the PKI it is most convenient or suitable in an environment with stakeholders with similar agendas. This has resulted in several new PKI developments for specific purposes, within one industry or one vertical such as healthcare. Some Member States have tried to incorporate vertical needs with an all-purpose PKI solution, such as the Austrian eID card with so called sector specific certificates (http://ec.europa.eu/idabc/en/document/4486/5584).

From the CIA (Confidentiality, Integrity, Availability) triangle public key cryptography provides confidentiality and integrity. The modern world however has more requirements in environments where sensitive information is being exchanged. It is not enough to know identity of the entity trying to access the information, but to also know the entity permissions or privileges regarding the requested resource. The authorization process grants the user specific permissions to e.g. access, modify or delete resources. A pure PKI does not allow us to build complex authorization policies, and therefore some of the Member States have built (authentication and) authorization solutions on top of existing authentication infrastructures, especially in the eGovernment sector. The scientific community has also tried to solve this issue by creating extensions to the basic PKI concept, and some of these concepts have been successful.

Another problem with large scales systems is the key distribution. Managing a large number of keys using a central solution such as PKI has proven to be problematic in certain conditions. Either there are tradeoffs in security, or problems with application support.

The last issue deals with public key cryptography itself. Current cryptography relies on the fact that it provides enough security based on availability of the resources, i.e. computational power. New approaches have been introduced both scientifically and commercially by moving away from the mathematics to other areas such as quantum mechanics.

This paper is a quick review on some of the existing systems and their benefits and inherent challenges as well as a short introduction to new developments in the areas of authentication, authorization and key distribution.

Definition of Trust Networks

There are several different approaches to build trust networks in an environment, where the participants are distributed both globally and operate perhaps in different fields or industries. Therefore it is required that we first define the basic terminology behind the term “Trust network”.

Definition of Trust

The term “Trust” can be defined in multiple ways depending on the viewpoint of the user. For our purposes we define the term in relation to information systems and security. The term has been already defined in several different scientific articles, so we will use the definition by [1]:

“Trust is the psychological state comprising (1) expectancy: the trustor expects a specific behavior of the trustee such as providing valid information or effectively performing cooperative actions; (2) belief: the trustor believes that expectancy is true, based on evidence of the trustee’s competence and goodwill; (3) willingness to be vulnerable: the trustor is willing to be vulnerable to that belief in a specific context where the information is used or the actions are applied.”

The above definition includes the important parties and functions in developing trust networks, i.e. the trusted party (trustee) and the trusting party (trustor) and the notion of vulnerability. From the definition we can see that vulnerability is a natural part of trust, and therefore we can further define that the confidentiality level of resources which are affected by the trust pose variable risk for the resource owner and possibly losses if the trust relationship is broken. The more confidential the resource, the more risk is placed on trust.

In computer security literature [6] the terms “Trust” and “Assurance” are typically related to technological concepts such as mechanisms, production methods or development process which purpose are to make sure that the system itself works properly. In this paper the term “Trust” however implies that a confidential resource is available to a trustee, and therefore can be understood as a legal or agreement level issue.

Trust Networks

Trust networks, or sometimes systems called “Web of Trust” consist of several different trusted and trusting parties. The relationships between the parties can be described as a mesh rather than a structural network based on hierarchies. In a typical trust network there are resources with variable levels of confidentiality. Even within one application / platform there can be multiple levels of functions or data resources that comply to different levels of confidentiality. The multiple participant, mesh structure and different levels of confidentiality make trust network concept a very complex issue.

For the purpose of this document we will define a trust network including these characteristics:

- Mesh of participants
- Some of the participants are trusted parties and some of the participants are trusting parties
- Each participant can act as a trusting and trusted party
- Trust relationship can be unidirectional or bidirectional
- There are one or more confidentiality levels of resources
- Creating a trust relationship means that the parties are willingly accepting a risk of actualization of a vulnerability [Please note that vulnerability does not mean software vulnerability but the unauthorized / wrongful use of a resource]

The most important feature of a trust network is the mesh –type of architecture. Hierarchical architectures are not in this sense networks, but can however be a part of a trust network as shown later

in this document. Because of the mesh structure the negotiation of trust between two different parties becomes a challenge.

Current Approaches

As mentioned before, there are several ways to implement a trust network. In this chapter we discuss some of the approaches in practise in the ICT world today. This is just a quick overview of the most used approaches and does not try to be exhaustive list of every available solution in use today.

PGP Trust networks (Web of Trust)

The PGP (Pretty Good Privacy) and especially OpenPGP (IETF specification RFC4880) is a way to provide message integrity, authenticity and confidentiality. [2] PGP keys are used to form a web or trust between the keyholders. To become a member of this web of trust the user needs a signature from a member of the desired web of trust. [3]

Examples

There are several examples of different type of PGP implementations and deployments of PGP. There are however no nationwide or even corporate wide use case examples available, or no examples were found during the limited time researching articles for this paper. The nature of PGP is more individual oriented and not organizational oriented. [3] Many OpenPGP based solutions can be viewed from the Wikipedia pages http://en.wikipedia.org/wiki/Pretty_Good_Privacy .

Standardization

Initially PGP was not standardized, but later on the developer of the PGP Phil Zimmermann both open sourced the PGP source code and started the standardization process. Now the latest version of the OpenPGP standard dates to November 2007, RFC 4880. The standard governing the usage of the PGP signed data is RFC 3156. The draft RFC 4880 is now a proposed Internet standard. [2]

Challenges

One of the challenges obvious in PGP is the requirement of a dedicated software or PGP enabled plugin in your own software. Although OpenPGP is a recognized Internet standard draft, to enable the user to take advantage of the system, almost always a dedicated software installation is necessary. However, in the email applications the situation is slightly better as the email clients will support OpenPGP utilizing IETF standard RFC 3156.

Another challenge of OpenPGP is the target audience. PGP was originally developed by Phil Zimmermann for enhancing the security in the email and bulletin boards (BBS). The main use for PGP is still the enhancement of message exchange. Other use cases have emerged such as file encryption, but it is unclear how PGP would be suited for purposes other than message exchange and ecryption.

As far as this investigation has shown, the PGP key is tied to a persons email address. This could prove to be problematic in a situation where the users would like to retain their PGP keys after their services in a company have ended. This is however not a PGP issue only.

Challenge in PGP and somewhat also for the OpenPGP is the lack of central authority and key backup, or their limits. The traditional PGP utilized a personal trust system, where a trusted person in a possession of a PGP key was able to sign a key of a new PGP user. Therefore no central authority governing the key signing process existed. [3] OpenPGP however can utilize certification authority based concepts and modern PGP implementations can use key management servers, and the newest versions can also support trust signatures, but are limited only 3 different levels (0,1,2), where the lowest level corresponds personal signature and the highest (2) level corresponds a concept of a CA certificate. [2]

PGP however does not offer any kind of solutions for authorizing the user to access the resource. PGP can be used to encrypt data and provide repudiation services, and to some extent to authenticate the user. There are however no accepted ways to integrate PGP as an authentication method, let alone a solution to authorize a user to access a resource. Proof of concepts has however been built, but they require modifications to the actual solution (PGP). [4] Also PGP has been utilized as a part of a RBAC solution for Web applications, but in a role which has almost nothing to do with the actual user authentication or authorization. [5]

PKI Solutions

The concept of PKI has been around for years, and is based on public key cryptography and key exchange algorithms created in the ’70s. [7] PKI has been touted to be the silver bullet for many security problems in the past, but hasn’t really been adopted widely until lately due to the EU Member State commitment to build infrastructures to help citizens conduct business with the government on-line. In the private sector PKI is typically used within one corporation for either limited use, or company wide. However during the quick research for this paper no examples were found around company wide PKI deployments. Not even the PKI vendors offer any case studies about company wide PKI deployments, nor PKI to PKI success stories (Bridge PKI). One of the biggest PKI deployments are the Common Access Card for the US military and several national PKIs deployed by governments both in EU and outside of EU.

There are 3 basic PKI deployment models as outlined in [8]. The traditional model is based on hierarchies, where a root CA will issue certificates for an arbitrary number of sub-CAs, and 1st level sub-CAs can issue certificates to 2nd level sub-CAs (depending on the path constraint rule) and so on. The second basic model is based on cross-certification between 2 different CAs, and can be described as a mesh model. In cross-certification the CAs will form a trust relationship where the CAs will trust the certificates issued by the trusted party (another CA). The third basic model is based on the concept of Bridge-CAs, where a specialized CA is deployed between 2 independent PKI deployments and acts as a trust broker between these 2 PKIs. EU Member state PKIs are in most cases based on the hierarchical model.

For critical environments Online Certificate Status Protocol (OCSP) plays an important part. Normally the certificate revocation status (is the certificate still valid) is checked from Certificate Revocation Lists (CRLs). In a typical scenario CRLs are however issued in intervals defined by the PKI configuration. This means that the certificate may have been revoked (compromised), but the information hasn’t reached the CRL yet as the next publishing event is some minutes away. OCSP was developed to answer this problem by providing an opportunity to request information about the certificate status through a separate protocol and responder. Depending on the responder the information can be timely correct, or still suffering from the CRL issuing problem. The CRL issuing problem is present in delegated OCSPs, where the responder actually provides information collected from several different CRLs (CAs) in a centralized manner.

Another important component in the PKI is the Registration Authority (RA) component. RA is used to delegate some of the key life cycle functions from the CA to a specialized component. RAs are typically subordinate to the CAs and provide offloading of some of the services such as certificate enrolment and key backup.

As a part of risk mitigation Time Stamping Protocol can be used in message exchange in the PKI.

An important thing to note about certificates is their categorization. [9] Certificates can be categorized using various kinds of approaches, but for this investigation we take into consideration identity certificates, where the public key of the certificate is tied to an identity of the entity, whereas the

second type ties the public key to attributes of the end entity. The latter certificate type is called an attribute certificate.

Examples

The most common use of PKI and certificates is web site / server authentication (https). This is something that every Internet user comes across on daily basis.

Many EU Member States have implemented national PKIs to enable certificate deployment to the citizens. For interoperability the Commission has launched a large scale pilot for enabling free movement of digital citizen identities across Member State borders: http://www.eid-stork.eu/.

From the private sector multiple use cases can be found, where PKI has been implemented for a specific, limited use case.

Standardization

For PKI there are several different standards, but the most important standards relate to key management and certificate validity checking. Key management does not mean just enrolment of the key, but the management of the whole life cycle of the key (and certificate). One of the first key management protocols was SCEP, Simple Certificate Enrolment Protocol developed by Cisco. SCEP is now an IETF draft (http://www.ietf.org/internet-drafts/draft-nourse-scep-17.txt). Another key lifecycle management protocol is CMP originally developed by PKI-Forum, later to be developed under OASIS when PKI-Forum joined OASIS and recognized now an IETF standard, RFC 4210. The competing standard with the CMP is Certificate Management of CMS (CMC), also an IETF standard RFC 5273. Both CMP and CMC utilize the IETF standard RFC 4211, Certificate Request Message Format (CRMF).

The IETF working group PKIX is responsible for multiple PKI related protocols and standards. For a security critical environment one of the important standards would be Online Certificate Status Protocol, OCSP, an IETF standard RFC2560 which will enable clients to receive up-to-date status information about the certificate validity, at least in theory.

Another important standardization body ITU-T is responsible for the actual certificate format, X.509. The actual specification has been adopted by other standardization organizations, and profiles of the specification are used to describe how the actual certificate format should be used. [9]

Challenges

PKI is typically built for hierarchical environments, i.e. as a response to an organizations or Member States needs for a particular use case. Although generic in nature, PKI adoption hasn't really grown to extensive networks. The most promising program to harmonize, or build interoperability between different PKI solutions is the STORK –project. The brief research showed that there are only a handful of operating trust networks based on PKI in existence, and even these are not general purpose networks for different types of organizations and stakeholders but rather networks between organizations operating in the same field or industry.

PKI infrastructure with all its components is complex. Deploying a PKI from the technical point of view is a simple task, but the problems arise in the management and policy part of the PKI. The issue is furthermore complicated by the lack of knowledge or experience in the user base. [8], [9] Cross-Certification has been deemed an issue coloured with political and self-interest issues, which are difficult to solve and may even have some technological implications [9]. The pkiC project in 2001-2002 clearly demonstrated how difficult it is to build interoperable PKI trust networks. [12]

Even though it was obvious early on that the actual driver of the PKI adoption must come from the application vendors and application users, the adoption of PKI standards has been frustratingly slow. Even today applications have a hard time dealing with certificates. The problems with applications is that the support must include the ability to process or parse the whole certificate information, check for validity either through CRLs or using OCSP, be able to construct the whole certificate chain and so on. The X.509 standard is complex and requires a lot of intelligence from the actual application. [8], [9]

The user certificates are static in nature. Once issued it is presumed that the certificate wouldn't have to re-issued within the next week or month. The mobility of the workforce poses a challenge here as new people replace current ones and old employees seek new challenges within the company or outside. [8]

For the critical systems information about certificate validity is of outmost importance. Without the ability to know the exact state of the certificate at any given time, the security of the system can be compromised. OCSP can mitigate the risk, but only when the OCSP actually has access to the real data of the certificate validity, and is not just a central point of issued CRLs. In applications OCSP support is still lacking, or not working properly. [8]

One identified problem in the past was discovered when eastern European countries built their own PKIs. The character sets used weren't compatible and resulted into problems. Character sets like UTF-8 were not used. [8]

The goal of the certificate is to identify its owner uniquely. For this purpose global namespace is used, but it has been seen problematic. [9]

PKI is expensive. The PKI core system itself can obtained for free using Open Source software, but the actual cost comes from the related and required components either software or hardware. Some of the requirements for the PKI result also in high costs of operation. [9] A recent study in Finland showed that of the 40 million Euros invested into different authentication solutions, the national PKI formed over 50% of the investment, and that there are only approximately 200 active users in whole of Finland using their eID card. [13]. Some legislations such as German Signature Law require ITSEC or CC evaluated products for producing qualified certificates which will further raise the cost of PKI. [9]

For PKI different implementations of EU directives might cause interoperability problems that need to be solved in an international trust network. [9]

To combat some of these challenges research and implementation has been made in the past [10], [11], but the results are modifications or new developments that are not standards compliant, and therefore not usable in the international landscape. They are however proofs that the usability of the PKI investments can be leveraged and show that even authorization models can be built on top the existing PKIs.

Identity Provider Driven Solutions (SAML, WS-)*

The Identity Provider (IdP) and Service Provider (SP) concepts were born in the wake of Web applications and application servers. Due to the complexities in several existing authentication methods IdPs and SPs were created to form an abstraction layer between the authentication source (PKI, LDAP Password, SMS, biometrics, OTP etc) and the actual service (application). For the application this means that it doesn't have to support its own identity repository, nor support various different authentication methods.

An Identity Provider is a solution that connects to various different user repositories and authentication sources and performs the actual user authentication on behalf of the application. The Service Provider

component resides close to the application, typically in the same application server and is used to intercept the service requests from the users and for verification that they have an authenticated session with the Identity Provider. The Service Providers in most cases offer the authentication and authorization information for the application using the application specific, application server specific or platform specific APIs. The native support for the platform / application / application server means that the integration effort for the application developer is typically measured in days, not weeks or months. E.g. the application can just ask "IsUserInRole()". All the complexities of the actual authentication as well as the initial authorization processes are hidden from the application.

Some IdP solutions can also perform authorization on behalf of the application during the authentication phase. The actual authorization can be considered to be happening in two phases. The first phase (optional) happens in the Identity Provider level. An IdP can have its own authorization policy based on various sources of information derived from either from the authentication method itself of the identity repository data. Users can be categorized based on the authentication method they chose, from attribute data derived during the authentication (reading e.g. certificate values), or more complex authorization schemes can be implemented. An IdP can combine the data from authentication with the repository data and make the authorization decision based on that information. A good example would be a case where a user authenticates using the national eID card. But as this is a corporate application, the data available during authentication is insufficient to make an authorization decision at the IdP level, so the IdP retrieves additional data from the identity repository such as corporate LDAP / Active Directory and determines that the owner of the certificate serial number XYZ belongs to a group of authorized users for this application.

Once the authentication and optional IdP level authorization is done, the user is redirected to the application, but now with an authenticated session. Within that session user attributes can be delivered to the application itself. These attributes are then used to authorize the user in the application level. An example of a set of application level authorization attributes can include

- Authentication method used (PKI, One-Time-Password, password, SMS etc)
- When the user was authenticated
- Which IdP authenticated the user (relevant if the application trusts several IdPs)
- Name of the user
- User role
- Etc…

In theory anything available to the IdP can be delivered to the application for the application level authorization. The ability to gather and deliver attribute information to the application from different data sources depends on the IdP implementation.

There are two general approaches how vendors have decided to implement the standards such as SAML 2.0. Either most of the intelligence is located at the IdP side, or the SP side (application) can include more functionalities. The standards themselves do not dictate how to implement the solution, but some interoperability requirements do require that the SP side is also capable of more complex tasks other than just intercepting service requests and delivering the received information to the application.

IdP Intelligence

Some IdP implementations have decided to create an intelligent IdP. Intelligence means that the IdP is capable of performing several different actions on behalf of the SP (application). These features are typically related to the processing of the information and combining the information from different sources. Another IdP related issue is authentication method management. In this case the authentication methods available to the SP are configured in the IdP level, and based on this

configuration, the user is presented an appropriate authentication method for that particular application, or a list of available authentication methods.

The major benefit in this approach is the fact that the SP side can be kept as simple as possible making the integration effort on the application side at its minimum. It also gives more centralized control within that identity domain to the administrators.

SP Intelligence

When more features and processing capabilities are implemented in a distributed manner, in the SP side, it can be said that the SPs are intelligent. The protocols used provide the means to request certain authentication methods from the IdP, making the SP an authority on how the user will be authenticated. The request may also be relative, i.e. the SP can request "authenticate this user using a method stronger / better than XYZ method"

From the application developer point of view this approach is more burdensome. The major benefit with this approach is that it works better in a situation, where the application trusts more than one IdP, and the application is located in a different identity domain than the IdP, i.e. the application is not under direct control of the IdP.

Identity Federation

The main purpose of developing Identity Providers (and Service Providers) was the desire to build standards based solutions in identity federation. Before explaining identity federation we need to define certain terms first.

- Identity Domain is an environment, where the identities are controlled by an independent Identity Provider

Identity federation happens when a users identity is transferred from one Identity Domain to another. For the user this is typically a Single Sign-On (SSO) operation.

From the standards point of view there are several mechanisms to achieve identity federation. The practicality however has shaped the available solution to adopt a subset of the standard itself. The most common ways are:

- The user exists in both domains and has the same attribute used to authenticate the user, e.g. UID
- The user exists in both domains, but the attribute used for authentication is different.
    - Upon first entry in the new domain, authentication and account linking happens
- The user does not exist in the trusting (receiving) domain.
    - A new account is created or
    - Transient federation is used

These are the basic ways how the user identity travels from one domain to the other. There are however much more functions that are executed by the IdPs in a trust relationship than those few examples above.

The trust between the IdPs are formed by exchanging Metadata files. These files are basically like certificates, but they also tell which kind of information can be expected from the other party. For the trusting party the trust relationship is like an authentication method, and for the trusted party the trusting party is like an SP.

If we look at the trust network definitions we established in the beginning of this paper we can see a lot of similarities between the trust network definition and identity federation. In federation trust relationships can be unidirectional or bidirectional, trust is formed based on exchange of metadata (and

agreements), the goal is to grant access to resources to external stakeholders, and relationships are formed between independent IdPs thus creating a mesh structure.

Examples

Large university trust networks has been built using an Open Source implementation of SAML 2.0. The system called Shibboleth is in use in most Finnish universities as well as in other countries. The system provides SSO functionality across university borders for the students and teachers.

Denmark has decided to use SAML 2.0 standard for all its eGovernment eServices [32]:

The largest authentication portal in Finland (www.tunnistus.fi), serving up to 10% of the population each month uses SAML 2.0 to connect different government agencies under a single authentication and authorization portal. Furthermore the Finnish government has taken the same approach in government electronic services as Denmark and has started to create a policy which mandates that the eGovernment applications and services should adopt SAML 2.0 standard for user authentication, authorization, and federation [31].

More references / examples can be found from www.projectliberty.org.

Standardization

The field of Identity Federation has two competing standards. SAML 2.0 is being developed by OASIS and WS-* based standards are developed by a coalition of industry players such as Microsoft and IBM. The standards overlap somewhat as WS-* implementations can utilize SAML assertions, but the protocols are different.

Project Liberty (www.projectliberty.org) is coalition of industry players trying to promote and profile the SAML standard. One of the most important tasks Liberty implements are the interoperability tests between different vendors and implementations of the standard. During these interoperability tests products and solutions are tested and if found interoperable, given a certification.

Challenges

As with PKI Identity Federation solutions are not interoperable out-of-the-box. Interoperability testing such as Liberty tests can help organizations choose products and solutions, open source or commercial, that can interoperate between each other, but still the solutions are not immediately interoperable.

The standards are still maturing, and the problem of two competing standards still remain. The standards are also general in nature, so standard profiling is necessary to guide all the participants in the trust network to implement their systems the correct way. This has happened at least in Denmark and in Finland in the governmental sector [31][32].

The biggest problem however is the fact that these standards and their implementations are for web based applications (browsers or Web Services). Integrating legacy applications may require more than just configuration work.

Each client platform would need an implementation of the protocol stack. Modern application servers such as BEA WebLogic have taken steps to integrate e.g. SAML 2.0 functionality into their products, but in general each platform may require their own implementation unless proxies are used.

The competing standards, SAML 2.0 and WS-* are created for similar purposes, but do not interoperate. They have converged somewhat during the past few years, but they are still quite different when comparing the actual protocols. Due to the Microsoft support for the WS-* protocol, SAML 2.0 protocol support for the vendors platforms (IIS, ASP.NET etc) lie in the third party support.

This is however only a problem, when a single protocol is chosen as a preferred way of exchanging identity information. Advanced IdP implementation typically support both protocols, and therefore sometimes acting as bridge between two different technologies within the identity domain.

New Developments

In this section new development efforts are described. New approaches to simplify PKI, apply new approaches using current technologies and creating completely new systems in the field of information security are briefly explained below. The developments selected here represent only a handful of possible remedies to current challenges.

Quantum Cryptography (Quantum Key Distribution, QKD)

Although quantum cryptography in itself is not yet possible without the quantum computers, quantum key distribution (QKD) is already real. Extensive studies have been conducted in the field of QKD and protocols created as early as in 1984 to enable secure key exchange between 2 parties [18], [19]. Also commercial appliances and applications have been built around QKD [17]. In October 2008 a highly publicized opening of a commercial network relying on QKD happened in Vienna. [16]

QKD can be used to replace public key cryptography so that the communicating parties can securely exchange the symmetric keys used in traditional cryptography for securing the data channel. The QKD is explained in greater detail in [18],[19],[20]. The main idea of QKD is to use quantum mechanics instead of computational complexity in key exchange. Instead of calculating something, the communicating parties use quantum communication channel to send qubits (typically using photons), which are then measured by the receiving party. The security of the QKD relies on the fact that one can not measure a qubit without disturbing its state, therefore making detection of eavesdropping possible at all times. In current quantum cryptography quantum communication channels are used only to exchange session keys.

The cryptosystem therefore relies on both quantum cryptography (key exchange, QKD) and traditional symmetric cryptography (securing the data channel). In addition to the benefit of the actual key exchange security there's also the risk mitigation factor that the key exchange channel and the data channel are separated from each other. In order to break the confidentiality or integrity of the exchanged information, the attacker would need to have access to both channels.

The security of the protocol and technology itself has so far been unbreakable, i.e. interception can always be detected. There are however ways to circumvent the security of the QKD by other type of attacks instead of eavesdropping. One of the most viable attacks for certain type of QKD systems is called a Photon Number Splitting attack (PNS). Single photon systems are not vulnerable to this attack, but unfortunately single photon systems are more expensive and harder to implement. The attack itself is quite improbable and hard to implement, but nonetheless poses a threat. Protocol modifications and detection mechanisms have been developed to detect this type of attacks. PNS and other type of attacks are explained in more detail in [19].

One of the greatest challenges in QKD is the establishment of ad-hoc connections. As man-in-the-middle (MITM) attacks are highly successful in QKD, there would have to be a mechanism to detect MITM attacks in a highly confidential network [18]. To mitigate this threat researches have suggested Quantum Key Distribution Protocols (QKDPs). The QKDP would be used to identify MITM attacks, but they still would need a similar approach that the traditional cryptography offers, i.e. reliance on a pre-known condition (a shared key or a shared state) [22]. However this approach does not rely on computational complexity, but rather to the quantum mechanics.

QKD is still in its infancy. Some commercial implementations (appliances) have been introduced to the market, but the technology itself is still very expensive and still under intensive research. Current technologies do not permit longer distances than 150km between 2 different parties in scientific experiments [18]. The communicating parties also need direct links between each other which makes QKD slightly problematic in geographically distributed systems with several different stakeholders,

i.e. in a mesh network. The detection technology would also benefit from improvements so that false positives in the interception detection could be minimized. False positives can happen when the noise in the communication channel grows and / or photons used to deliver the information lose their energy.

Because QKD is still very new technology we can not be sure that the implementations made today are secure also within the next couple of years. Already the QKD systems as a cryptosystem has been found to have security risks [21], but QKD still looks to be one of the most promising technologies for replacing public key cryptography for establishing sessions keys in highly confidential environments.

Identity Based Encryption System (IBE)

IBE takes a new approach on public key cryptography and especially key distribution. With IBE systems it is not necessary to perform complex certificate chain lookups or investigate CRLs. IBE systems can be easily, at least in concept level, be developed for Java applications. [14] Identity Based Encryption was first proposed by Adi Shamir [27], [28] and the first usable algorithm was made available in 2001. [28]

IBEs basic idea is to use a known attribute as the public key of the user [26]. The public key can be something the other users can easily remember or obtain easily, such as an e-mail address. This public information is then used as the public key. The private keys are generated on demand basis by a Private Key Generator (PKG). The PKG is responsible for generating the private keys for all the participating users within the system. In the most simple form the data is encrypted using the public key derived from the public information and the receiver can decrypt it by requesting a private key from the PKG. An additional benefit of this system is that qualifying information can be appended to the public information, such as validity period. This would make e.g. short lived message validity periods possible when exchanging confidential information between two parties, but information which is considered obsolete within a short period of time.

IBE removes one of the biggest problems of traditional PKIs, certificate enrolment, revocation (and subsequent CRL challenges) and provides means to securely exchange information between two parties without previous knowledge (a certificate). But, as in all systems, there are tradeoffs. In the IBE system the PKG will be the most vulnerable part, and should also be the most trusted part as the PKG is able to decrypt all the messages sent between the communicating parties as the PKG is responsible for generating the private keys. IBE poses also other problems both from technical and legal point of views. Key revocation e.g. is a concept not known to pure IBE systems. Key revocation in the IBE system would mean identity revocation: revocation of the identity information used to create public keys for identities. EU directives also dictate that the private key should be in the possession of the user, and only the user, which is not the case with IBE.

The rapid adoption of IBE has already made it a widely accepted solution in scenarios where the user base is not known, or dynamic in nature. It has also proceeded to standardization by the IETF (RFC 5091) [28].

SPKI/SDSI

The SPKI/SDSI is a system based on authorization certificates instead of traditional identity certificates [25]. The SPKI was created to address the global namespace problem and authorization problem of traditional X.509 certificates [29]. Either the global namespace concept provided too much collisions (How many Tony Blairs), or the global names were meaningless. SPKI/SDSI enables a resource owner to define his own namespace and through the use of the resource owners key global names, but without loosing the local meaningfulness.

Another aspect of SPKI/SDSI is the authorization function [25]. With SPKI/SDSI system the resource owner can tie authorization to use the resource to a public key and even include the possibility to

delegate this permission / authorization further. Each delegate could (if allowed) to create further delegations by issuing authorization certificates. In SPKI/SDSI each entity can act as a certificate issuing entity.

SPKI/SDSI is currently more of a scientific interest and not a viable commercial concept. The adoption of SPKI/SDSI has not taken off [9].

Key-Policy Attribute-Based Encryption

The paper [30] presents yet another approach how to manage and create a cryptosystem to protect sensitive data by extending previously presented solutions (such as IBE, and Attribute Based Encryption, ABE). Key-Policy Attribute-Based Encryption (KP-ABE) tries to resolve issues where access to sensitive data should be allowed based on authorization, not authentication, and that the data in storage should be protected against unauthorized access (confidentiality).

The authorization functions in KB-ABE allow the resource owner to grant access in fine-grained level to certain keyholder by associating an authorization structure to the key. If the permissions set of the resource match the authorization structure of the keyholder, he can access the resource (decrypt). The system also has SPKI/SDSI reminiscent functions where a keyholder can generate new keypairs and delegate these to other entities acting as local key authorities.

Conclusions

The amount of available information is growing constantly. Majority of the information generated is public in nature, and therefore does not require protection. Some of the information however is sensitive or confidential in nature and requires protection. When the information or assets are in an electronic form, we need to build safeguards to protect them against different kinds of risks.

The growing amount of information is also related to the growing number of interconnected systems. Within an industry or government there's a constant struggle to create as safe as possible systems which can still be used in a connected manner. Each system that gets connected to other systems is vulnerable to exploits, inside or outside. The connections created between systems create networks where trust need to established.

The most known and researched way of implementing trust between system relies on public key infrastructure (PKI). Due to the maturity of the PKI and research done in that area we can in adequate confidence say that we have acknowledged the benefits and challenges in PKI. The area of PKI is standardized and hasn't seen any radical changes lately. It's proven technology. But the proofs have also shown that PKI is most suited for specific needs, and even though it is thoroughly standardized big interoperation problems still exist. For the modern application processing the sensitive data PKI does not offer easy ways to implement authorization. Majority of the certificates in circulation today are identity certificates, which are best used for authentication but unfortunately do not offer flexible authorization schemes that could be adapted to our dynamic, ever changing environment.

Extensions or new concepts to PKI include such efforts as SPKI/SDSI and Identity Based Encryption. From the application standpoint they are however immature and only IBE has seen wider commercial success. Building large trust networks is not feasible with either solution as there's no standardization, lack of application support or that they are a poor fit for the actual needs of strong authentication and authorization.

For modern web based applications, either browser based or Web Service based, a combination of a strong authentication mechanism and authorization management system will provide the best possibilities to ensure the confidentiality of information without limiting the availability too much. Standards such as SAML 2.0, WS-Federation and Identity Provider products provide the abstraction layer in authentication and authorization to these applications and integration can be done using the native tools of the platform, such as Java, .NET etc.

Only during the couple of last years have we seen a completely new way of creating trust networks. The quantum key exchange makes it possible to exchange the symmetric encryptions keys in a completely new way. Instead of relying on computational complexity QKD leverages the scientific breakthroughs in quantum mechanics and cryptography, i.e. the ability to code information using photons. So far the protocols and the technology seem impervious to traditional type of attacks. However quantum cryptography is still in its infancy and can not be considered to be used in a wide spread manner. It is interesting to see if this technology develops into a level where the actual devices are cost effective, interoperable and reliable so that they can provide new means of creating trust networks.

In conclusion we can state that there are a lot of alternatives when we need to create trust relationships between different stakeholders and in creating trust networks (mesh). None of the alternatives provides an all compassing solution. All the options have their strengths and weaknesses. So far the most promising way of delivering manageable and deployable solution to trust relationship building that includes strong authentication from various sources and authorization management comes from the IdP

approach when an existing authentication source is combined with the possible authorization management functions offered by the IdP.

References

[1] J.Huang, M.S.Fox (2006), “An Ontology of Trust – Formal Semantics and Transitivity”, ICEC’06, August 14-16

[2] http://en.wikipedia.org/wiki/Pretty_Good_Privacy

[3] D.Henry (1999), ”Who’s Got the Key?”**,** SIGUCCS '99: Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations

[4] M.D. Corner, B.D. Noble (2003), “Protecting Applications with Transient Authentication”, Proceedings of MobiSys 2003, San Francisco, CA, USA May 5-8

[5] J. S. Park, R. Sandhu, G-J Ahn (2001), “Role-Based Access on the Web”, ACM Transactions on Information and System Security, Vol. 4, No. 1, Pages 37–71.

[6] http://nob.cs.ucdavis.edu/book/book-aands/aands01.pdf

[7] http://en.wikipedia.org/wiki/Public_key_infrastructure

[8] A. Lioy, M.Mariam, N.Moltchanova, M. Pala (2006), “PKI Past, Present and Future”, International Journal of Information Security 5, pages 18-29

[9] J.Lopez, R.Oppliger, G. Pernul (2005), “Why have public key infrastructures failed so far?”, Internet Research Vol. 15 no. 5

[10] M. R. Thompson, A. Essiari, S. Mudumbai (2003), “Certificate-Based Authorization Policy in a PKI Environment” ACM Transactions on Information and System Security (TISSEC), Volume 6 Issue 4

[11] J. Lopez, A. Ma˜na, J. A. Montenegro, J. J. Ortega “PKI design based on the use of on-line certification authorities”, International Journal of Information Security, Vol. 2 Issue 2, p91-102

[12] http://eema.org/downloads/security_finished_papers/pkiC_final_report.pdf

[13] http://www.vtv.fi/chapter_images/8463_161_2008_Tunnistuspalvelut_NETTI.pdf

[14] L. Owens A. Duffy, T.Dowling (2004), ”An Identity Based Encryption System”, PPPJ '04: Proceedings of the 3rd international symposium on Principles and practice of programming in Java

[15] T. Stading (2003), “Secure communication in a distributed system using identity based encryption”, Cluster Computing and the Grid, 2003. Proceedings. CCGrid 2003. 3rd IEEE/ACM International Symposium

[16] http://news.bbc.co.uk/2/hi/science/nature/7661311.stm

[17] S.K. Moore (2007), “Commercializing Quantum Keys”, IEEE Spectrum

[18] http://en.wikipedia.org/wiki/QKD

[19] K. Inoue (2006), “Quantum Key Distribution Technologies”, IEEE Journal of Selected Topics in Quantum Electronics, Vol. 12, No. 4

[20] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, B.C. Wang (2005), “Comparison of Four Multi-User Quantum Key Distribution Schemes Over Passive Optical Networks”, Journal of Lightwave Technology , Vol. 23, No. 1

[21] J. Cederlöf and Jan-Åke Larsson (2008), “Security Aspects of the Authentication Used in Quantum Cryptography”, IEEE Transactions on Information Theory, Vol. 54, No. 4

[22] T. Hwang, Kuo-Chang Lee, and Chuan-Ming Li (2007), “Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols”, IEEE Transactions on Dependable and Secure Computing, VOL. 4, NO. 1

[23] A. Ganesh, K. Gopinath (2008), “SPKI/SDSI Certificate Chain Discovery with Generic Constraints”, ACM

[24] http://en.wikipedia.org/wiki/SPKI

[25] ftp://ftp.isi.edu/in-notes/rfc2693.txt

[26] http://en.wikipedia.org/wiki/Identity-based_encryption

[27] http://middleware.internet2.edu/pki05/proceedings/callas-conventional_ibe-presentation.pdf

[28] L. Martin (2008), “Identity-Based Encryption Comes of Age”, IEEE Computer Vol 41, Issue 8, pages 93-95

[29] C.M. Ellison (1999), “The Nature of Useable PKI”, Computer Networks, Volume 31, Issue 8, pages 823-830

[30] V. Goyal, O. Pandey, A. Sahai, B. Waters, CCS '06: Proceedings of the 13th ACM conference on Computer and communications security, October 2006

[31] http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20080421Virtul/03_suunnitteluohje-20080412.pdf

[32] http://www.projectliberty.org/liberty/content/download/3789/25018/file/Danish%20Public%20Sector%20Federation-Nielson%20071023.pdf

European Commission

EUR 23774 EN– Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Building Trust Networks
Author(s): Petteri Ihalainen
Luxembourg: Office for Official Publications of the European Communities
2009 – 24 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-11631-5
DOI 10.2788/82918

Abstract
The common agreement in the industry is that the Public Key Infrastructure is complex and expensive. From the year 1976 with the introduction of public key cryptography and the introduction of PKI concept in 1977 a lot of scientific resources has been spent on creation of usable key exchange systems and concepts to build trust networks.

Most EU Member States have implemented their own national Public Key Infrastructure solutions mainly to enable strong authentication of citizens. They are however not the only systems within the EU to utilize PKI. Due to the nature of the PKI it is most convenient or suitable in an environment with stakeholders with similar agendas. This has resulted in several new PKI developments for specific purposes, within one industry or one vertical such as healthcare. Some Member States have tried to incorporate vertical needs with an all-purpose PKI solution, such as the Austrian eID card with so called sector specific certificates (http://ec.europa.eu/idabc/en/document/4486/5584).

From the CIA (Confidentiality, Integrity, Availability) triangle public key cryptography provides confidentiality and integrity. The modern world however has more requirements in environments where sensitive information is being exchanged. It is not enough to know identity of the entity trying to access the information, but to also know the entity permissions or privileges regarding the requested resource. The authorization process grants the user specific permissions to e.g. access, modify or delete resources. A pure PKI does not allow us to build complex authorization policies, and therefore some of the Member States have built (authentication and) authorization solutions on top of existing authentication infrastructures, especially in the eGovernment sector. The scientific community has also tried to solve this issue by creating extensions to the basic PKI concept, and some of these concepts have been successful.

Another problem with large scales systems is the key distribution. Managing a large number of keys using a central solution such as PKI has proven to be problematic in certain conditions. Either there are tradeoffs in security, or problems with application support.

The last issue deals with public key cryptography itself. Current cryptography relies on the fact that it provides enough security based on availability of the resources, i.e. computational power. New approaches have been introduced both scientifically and commercially by moving away from the mathematics to other areas such as quantum mechanics.

This paper is a quick review on some of the existing systems and their benefits and inherent challenges as well as a short introduction to new developments in the areas of authentication, authorization and key distribution.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LB-NA-23774-EN-C

ISBN 978-92-79-11631-5