Dokument	introductiontopki
Author	Simon Wiberg, Stockholms universitet
Identifier	
Version	1.0.0
Last Modified	2006-09-25 10.35
Status	Published

Introduction to Public Key Infrastructure

SwUPKI is the public key infrastructure for the Swedish higher education community. SwUPKI is an established service within SWAMI, the Swedish Alliance for Middleware Infrastructure.

This PKI tutorial is primarily written for IT-professionals at universities who are considering joining SwUPKI. The intention is to give a general description of the usefulness of a public key infrastructure (PKI), and to give an overview of how PKI works. SwUPKI is not described in particular here.

The Usefulness of PKI

A PKI can be used to securely verify the identity of senders and receivers of data transmitted over networks. The PKI can also be used by the receiving party to verify that the data sent has not been intersected and tampered with.

This can be useful in communication between people, by email for example. A PKI can also be used for authentication[1] to systems and applications. The entities that are authenticated can be either individuals or other systems or applications. For simplicity we will here refer to all these as entities.

In an IT-environment based on middleware infrastructure, there are a lot of interactions between systems and applications. It is vital to protect the integrity of the information in these transactions and verify the identities of the parties to the transactions. For example, many resources will interact with the enterprise directory. Information in the enterprise directory might at the same time govern user permissions in, for example, the business systems. Breaches in security for the transactions with the enterprise directory could therefore be very serious.

A PKI is basically a hierarchy of trust. The dynamic is that the members of a PKI trust an agent in the top of the hierarchy, and more important the members trust those who are trusted by the agent. Thereby the members do not have to establish trust between each other in order to be able to engage in secure communications between each other.

To understand how this works one must first understand the methods used to verify the identities of entities involved in information transactions, and to verify that transmitted information has not been tampered with. We will cover these methods first and then describe the organisation of PKI.

Cryptography – the Fundament of PKI

PKIs rely on cryptography to verify identities and protect the integrity of data. Here we will briefly describe the principles of secret and public key cryptography.

The traditional form of cryptography is based on the use of one secret key. This key is used to encrypt data to an unreadable format. To decrypt the data, back to readable format, the same key must be used. This form of cryptography is known as *secret* key cryptography or symmetrical key cryptography.

In *public key cryptography*, as opposed to secret key cryptography, a set of two keys are used. The keys are linked in such a way that what is encrypted with one key can only be decrypted with the other key. Both keys can be used to encrypt and decrypt data, but what is encrypted with key A must be decrypted with key B and vice versa. A recipient of data can make one of the keys publicly available and keep the other key secret. A sender of data can then encrypt data with the recipient's public key and this data can only be decrypted and read by the recipient with the secret key.

The technique can also be used the other way around. Assume that the sender of data also has a pair of keys – one secret and one publicly available. The sender could then encrypt the data with the secret key. Anyone intersecting the data could then, knowing who the sender is, decrypt the data with the public key. However, if the data can be decrypted with the sender's public key, one can be certain that it has been encrypted with the sender's secret key. So if the data can be decrypted with the sender's public key, the recipient can be certain that the sender is who he/she/it claims to be, and that the message has not been tampered with.. That is under the assumptions that the recipient can trust that the sender's secret key is actually secret and that the public key actually belongs to the sender. These trust issues are of crucial importance in a PKI, we will elaborate on that later on.

From the examples in these two paragraphs it should be evident that cryptography can be used both for keeping unauthorised people from being able to read data, and for the purpose of verifying the identity of the sender of data. From now on we will focus on the latter of these two uses of cryptography.

Digital Signatures

With a digital signature it is possible to verify the identity of the sender of data and also to verify that the data has not been manipulated by a third party. A digital signature is a code attached to the transmitted data.

It works like this. Before sending the data, a code (known as a hash) is constructed from the data by a recognised formula. The formula is such that it is extremely unlikely that any other data would give the same hash. After the hash is constructed, it is encrypted with the sender's secret key and attached to the data.

When receiving the data, the receiver also constructs a hash from the data. The receiver also decrypts the attached hash with the sender's public key. If these two hashes are equal, the receiver of the data has verified the claimed

identity of the sender and will also know that the data has not been manipulated by anyone else. That is, once again, under the assumptions that the sender’s secret key is actually secret and that the public key actually belongs to the sender.

PKI Organisation

Above we have covered some of the basic methods for using public key cryptography in computerised communication. We will now focus on PKI organisation. A natural place to start is to ask: why is there a need for an organisational framework to use public key cryptography?

One could imagine using the methods described here for signing and verifying data. Those exchanging encrypted data or digitally signed messages would then have to come to bilateral agreements about how to exchange public keys, what hash formulas to use and other details. This does not scale very well. The dynamic of PKI is that it eliminates the need for bilateral agreements among each of the members.

Digital Certificates

For the uses of public key cryptography described above, it is crucial that the public keys can be tied to specific entities. An important part of the PKI is the certificate authority (CA). The CA issues certificates that, based on the trust for the CA, prove that a certain public key belongs to a certain entity. The certificate itself is a digital document with information about the entity that holds a certain pair of keys, the entity’s public key is also included in the certificate. The certificate is digitally signed with the CA’s secret key. The certificates are (normally) publicly available. This means that the members of the certificate community can check the authenticity of each others digital signatures. To be able to verify the certificates, the CA’s public key must be distributed in a secure way to the members of the PKI.

Hierachy of CAs

A PKI does not necessarily consist of just one CA, the certified members of the PKI can in many cases issue their own certificates. This means that their can be a hierarchy of CAs in a PKI. The top level CA is then referred to as the root CA or Policy CA (PCA). The member of the PKI has a public key that is certified by the PCA, the member also has the matching secret key. When a member CA issues a certificate, it signs the certificate with its secret key. Verifying a transaction signed with a member generated secret key is a three step process like follows, but not necessarily in that order.

1. Verify the signature with the public key for the member certified entity.

2. Verify the signature of the member issued certificate with the public key for the PKI member to ascertain that the correct public key is used in step 1.

3. Verify the signature of the of the PKI member certificate with the public key for the PCA.

In this way there is a trust path from any certificate in the PKI up to the PCA's own certificate. This certificate is signed by the PCA itself and is the only certificate in the PKI that cannot be validated within the system, but has to be

checked and validated by other means. Theoretically at least, there is no end to how many levels of CAs there could be in a PKI. In SwUPKI the members run there own CAs and issue certificates for there local needs.

Certificate Policy

The certificate policy is the fundamental mission statement for the PKI. The policy is aimed both towards potential members as well as external partners.

To build confidence in the PKI, the policy should declare what ambition the PKI has for the security level of its services. The methods used to achieve this should also be declared. The obligations of the CA and other parts of the PKI organisation should be described. Further, the conditions and rules for membership should be described, and the routines for issue and revocation of certificates. The policy should also describe the applicability of the certificates that the PKI issues.

Certificate Authority (CA)

The CA (PCA or root CA if there are also member CAs in the PKI) is the part of the PKI organisation that is primarily responsible for the practical running of the PKI. The CA handles the key distribution and also issues and publishes certificates. Further the CA is responsible for publishing certificate revocation lists (CRLs). The practices of the CA must inspire trust. In order for the users to trust the certificates, they must have trust for the CA.

Certificate Practice Statement (CPS)

In the CPSs the members of the PKI declare how they use the certificates in their particular IT-environments. Particular attention is typically paid to how secret keys are stored and handled. If the PKI members can themselves issue certificates, a lot of the CPS will focus on the organisation, methods and routines for this

Policy Management Authority (PMA)

PKI organisation might differ somewhat, in some PKIs are the administration of membership requests and policy issues separated from the more hands-on running of the PKI. This is the case in SwUPKI for example. In SwUPKI is the administrative functions handled by the Policy Management Authority. Their duties include examining proposed CPSs to ascertain if they comply with the Certificate Policy. The PMA also examine if the members follow the routines and so forth specified in their CPS. If or when members do not act in accordance with the certificate policy or their CPS, the PMA is responsible for deciding on appropriate actions. In such a case the first step would most likely be to tell the member concerned to adjust their practices, and if they do not, their membership in the PKI could eventually be revoked by the PMA. The PMA is also an important part in building and maintaining the trust in the PKI.

---

[1] Authentication is a mechanism through which an individual or resource can prove his/her/its claimed identity when accessing a protected resource.