Glück Kanja

Using OpenPGP in Corporations

Abstract

Due to a commonly limited understanding of the OpenPGP PKI's structure and its possibilities, the OpenPGP Trust Model is still considered to be suitable for private use only by security advisors. This White Paper will clear up any misunderstandings and show that the OpenPGP and X.509 concepts are actually quite similar.

Type: Technical White Paper

Last Changed: April 12, 2002

Clearance: Public

Table of Contents

Facts

The Origin

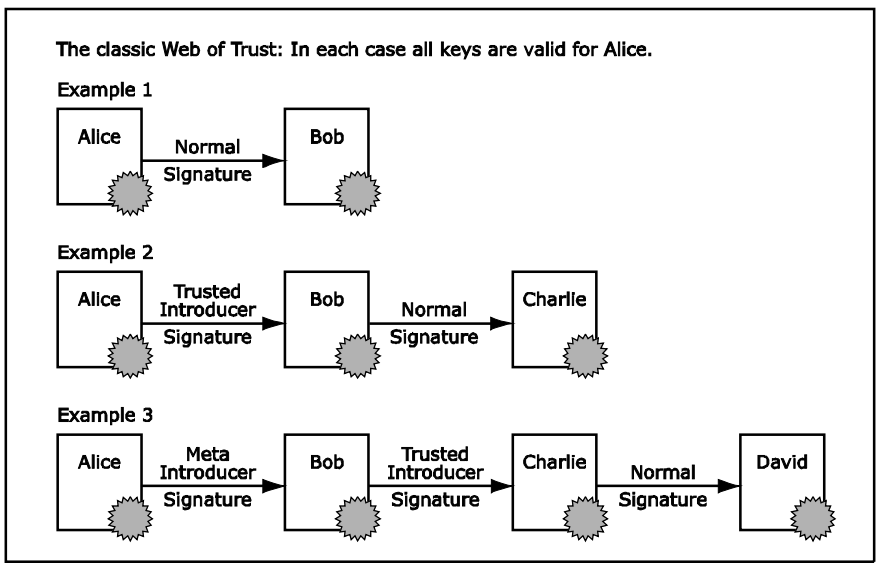
OpenPGP Web of Trust

To be able to comprehend the following concept, it is important to completely understand the OpenPGP Web of Trust. OpenPGP was originally designed for the Internet community, whereas X.509 was designed for a hierarchal structure. While the X.509 concept requires a certification authority (CA) that the user can trust, OpenPGP thinks of each user as its own CA. In other words, X.509 begins the chain of trust with the CA, whereas OpenPGP begins with the user himself.

The Web of Trust is based on the theory that every person is somehow connected to every other person through a very limited number of people. The OpenPGP concept uses this theory to construct the chain of trust.

A simple example: *Alice and Bob both have an OpenPGP key. Alice meets with Bob and signs his public key. This now makes Bob's key valid for Alice. This single level certification is the simplest case.*

With this signature, Alice can also indicate if she wants to trust additional keys signed by Bob. In this case, Alice would sign Bob's key as a so-called Trusted Introducer. If Bob then signs Charlie's key, Charlie's key will also become valid for Alice. This is called transitive trust.



The Web of Trust allows even more complex situations: *Alice signs Bob's key as a so-called Meta Introducer, which means that Bob can make other keys valid for Alice, but he can also turn other keys into Trusted Introducers for Alice. To do this, Bob must sign Charlie's key as a Trusted Introducer. If Charlie signs David's key, David's key would then become valid for Alice.*

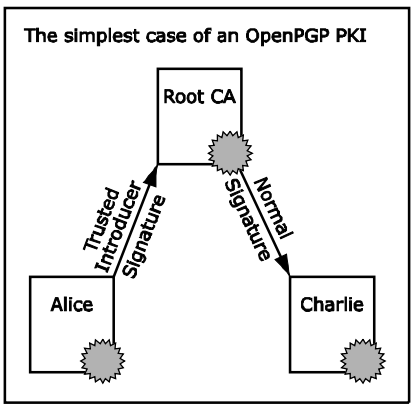
These examples present the simplest, linear case. Trust and validity is, however, spread not only through Alice, but also through every user. This creates a star-type, multilevel connection. Please note that key validity in the Web of Trust can only be calculated in context of the user.

Although this model is very academic, it is surprisingly similar to the human trust feeling. Still, it is also understandable why companies are traditionally more likely to set up a hierarchal structure. The next section shows that the Web of Trust is actually a superset of a normal hierarchy.

Hierarchy as Limited Anarchy

Let's take another look at the second example with the two-step chain of trust:

Alice signs Bob's key with a Trusted Introducer Signature. Bob signs Charlie with a normal Signature. Charlie's key is now valid for Alice.



If we simply rename „Bob's Key" to "CA Key" the following situation occurs:

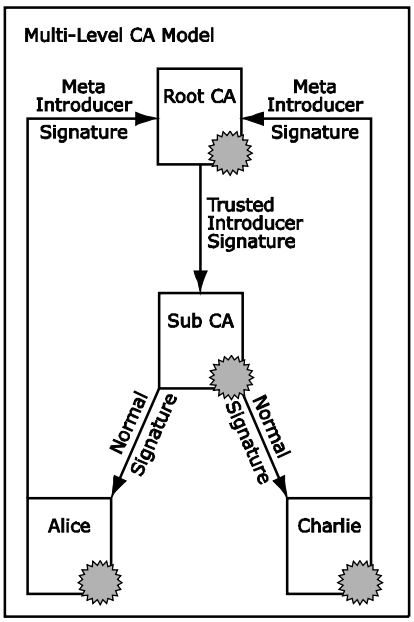
Alice signs the CA Key with a Trusted Introducer Signature. The CA signs Charlie with a normal signature. This now makes Charlie's key valid for Alice.

With this small change, a CA with a built-in hierarchy has been created, from a Web of Trust. This is the simplest form of a hierarchal OpenPGP PKI. The X.509 model looks exactly the same, with the exception that Alice must place the CA key in her Key Management rather than signing it.

It is important to understand that this model contains absolute conformity to the OpenPGP Standard, which means it is fully compatible to all the of the OpenPGP programs. The specific limitations of users within the individual enterprise are the focus, not the misuse of the Web of Trust. More on this subject later.

Expansion of the Basic Concept

Creating a Multi-Level PKI



A simple hierarchy, like the one mentioned in the example above, is not flexible enough for most scenarios. Therefore, it makes sense to introduce a further level, for example, dividing the place of certification into a Root CA and a Sub CA. An example:

Alice signs the Root CA as a Meta Introducer. The Root CA signs the Sub CA as a Trusted Introducer. This signs David with a normal signature. This makes David's key valid for Alice.

If this certification chain goes in both directions, David and Alice will recognize each other's keys

More Sub CAs

It is also possible to smoothly integrate more than one Sub CA, for example to take care of international business locations of a corporation, each one having their own Sub CA. It is advisable to store the Root CA in a physically and electronically safe environment while the corporation creates its own operative Sub CA for every continent.

Cross-Certification

A cross-certification is easier and more flexible with OpenPGP than with X.509, since an OpenPGP key, unlike an X.509 certificate, can hold many signatures. To be able to trust another enterprise's user certificate, it is necessary to sign their Sub CA with one's own Root Certificate as a Trusted Introducer. The key, as well as the Sub CA of the partner enterprise, then carries the signature of their own Root CA as well as the signature of the Root CA of the partner enterprise. If required, this signature can have a certain validity of, for example, one year, after which it must be re-certified.

For the employees of an enterprise, the foreign Sub CA's signed keys and every key that is certified through this Sub CA will be automatically made valid. When both of the enterprises want to cancel the cross-certification, a revocation of the Trusted Introducer Signature through the Root CA is all that is needed.

Since OpenPGP supports many Root CAs, the certification of external partners and further Root CAs can be introduced.

External Partners

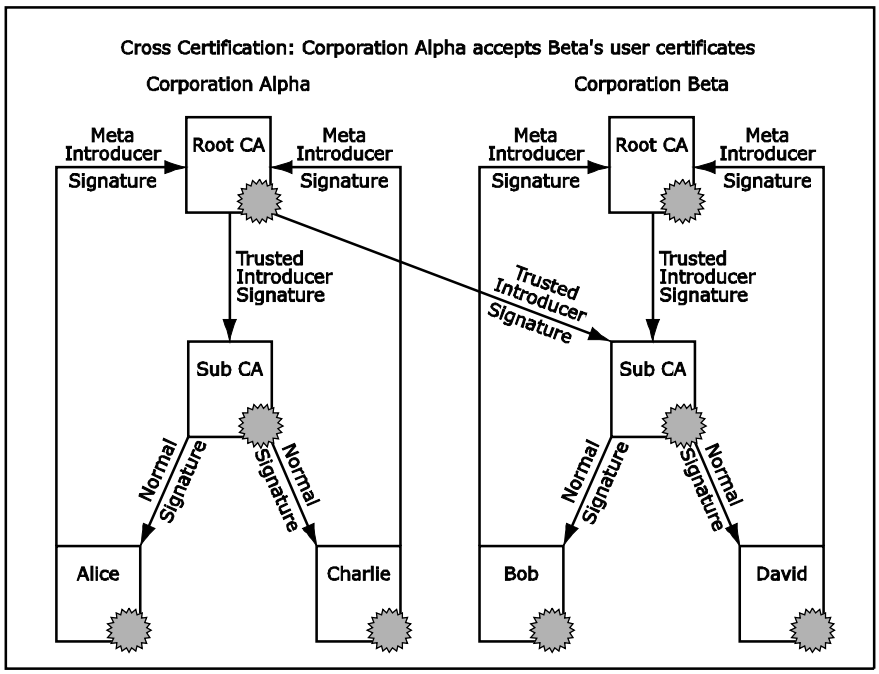
If not an entire enterprises are to be cross-certified as a whole, but external individuals are, it is sensible to introduce a Partner Sub CA. The Partner Sub CA

must be signed by the Root CA as a Trusted Introducer. The Partner Sub CA then certifies the external user directly.

Exclusion of External Webs of Trust

An external partner's possible Web of Trust has no influence on the internal PKI since the end user can only sign other keys with a normal signature, which has no transitive trust.

On the other hand, if an external user signs the Root CA or Sub CA of the enterprise, this only has an influence on the external Web of Trust, not on the Public Key Infrastructure of the enterprise. This case is also advantageous. If an external employee signs the Root CA of the enterprise as a Meta Introducer, all of the enterprise keys will be automatically valid for him and possibly additional parties who share a Web of Trust with the partner, without the enterprise having to take an active part.



It is important for the maintenance of the hierarchal PKI that the user be prohibited to import keys in the personal key ring that don't belong to the CA keys of the enterprise's PKI. By importing and signing foreign keys, the hierarchy would be watered down and the user's security application would not automatically recognize revocations.

Centralized Key Generation

Although a decentralized key generation is the traditional way with OpenPGP, a centralized generation for an enterprise is suggested for many different reasons. The keys can be generated in a safe environment. Also, user mistakes or problems are reduced. Furthermore, it can be assured that the keys are created in the right format with the right signature and that the public keys are made available in the PKI. A backup of the private key with a decentralized generation is hardly possible. However, a backup of the keys is recommended

for two reasons: recovery of the secret key and password and in case a user's employment ends and the company needs to access the encrypted data, and second in the case of loss of a key or password.

To make this type of Public Key Infrastructure possible, the key material, delivered to the user after the automatic generation, should look like this: The user's public key must be signed by the appropriate Sub CA so that the key appears as valid for other users in the PKI. The Root CA's and Sub CA's public keys must be included so that the user can check the validity of the keys from the PKI. Finally, all Root CA certificates contained in the users' keyrings must be signed as Meta Introducers – not on the server, but rather in context of the user. Now the user is PKI-enabled. This sequence of events can be automated in well-developed OpenPGP CAs.

By the way: Through central generation of OpenPGP keys, the same CA/RA structure is possible as with the generation of X.509 certificates.

X.500 Directory Service and Keyserver

The enterprise employees' public keys must be made available on a central server. OpenPGP offers two different infrastructure possibilities. First, there are HTTP servers which were called into existence in the early days of OpenPGP to provide a basic PKI component. It is advisable to use HTTP Keyservers if legacy clients and more exotic operating systems have to be supported. Keyservers manage the keys as a flat list and are not deeply integrated in the enterprise's infrastructure. This means that the keyserver presents a further database to be maintained in the enterprise. There is also the general problem of replicating keyservers to take care of a company's distributed sites.

Using an X.500 directory service is more elegant and much faster. Many enterprises already have available, or are currently working on the implementation of such a directory. It is possible to place OpenPGP certificates in an X.500 directory service and to access them using LDAP. This is suitable for most products that are currently available on the market such as Microsoft Active Directory, Siemens Dir.X Meta Directory, Netscape Directory Server or Novell NDS. It is recommended that the existing directory service be employed to prevent the need to create and take care of a further infrastructure (concept, service, replication, availability, backup, etc.).

When designing the directory schema, special consideration should be given so that more than one certificate can be assigned to a user. This is especially important, since revoked certificates should be included in the directory service, next to the current certificates. In addition, the Key ID should be placed in a separate field and indexed, since this property is specifically searched for during different client operations.

Summary

Although the classic Web of Trust is not suitable for enterprises, it can be formed to build a hierarchy while remaining standard-compliant. Using this concept, an enterprise can build a very flexible OpenPGP Public Key Infrastructure. For most of the enterprises a multi-level CA model is recommended. For more complex cross-certifications or the integration of

external partners, OpenPGP shows that it is more pragmatic and flexible than X.509, because OpenPGP keys can contain an unlimited number of signatures instead of only one in the X.509 world. The generation and certification of the key material should be centrally administered. Like X.509 certificates, OpenPGP keys should be stored in X.500 directory services.

For more information

For more information visit www.glueckkanja.com

For comments, questions and feedback on this white paper please send an e-mail to support@cryptoex.com.