PKI (Public Key Infrastructure), How it works.

Roger W. Younglove, CISSP

Sr. Network Security Consultant, NetCare Security Services, Lucent Technologies

Businesses today are increasingly looking to VPNs to provide cost-effective, secure communications services that will enable them to link their business processes more closely with partners, their supply chain, and even customers in ways never dreamed of just a few short years ago. Moreover, the prospect of replacing costly leased and dial-up lines with efficient IP connections to link remote workers and branch offices to the corporate network is a compelling business proposition for many organizations.

Using a combination of tunneling, encryption, authentication, and access control, a VPN gives users a secure method to access corporate network resources over the Internet or other public or private IP networks. Implementation of a VPN involves two major technologies: a tunneling protocol, and a method for authenticating users of the tunnel.

IPSec, a Layer 3 (Network Layer) tunneling protocol, is typically used today for encrypting and encapsulating data for secure transfer across VPNs in enterprise networks. A variety of authentication methods to verify the identity of valid users can be implemented with IPSec, including shared secret, token cards or digital certificates. For a large extranet implementation, the easiest method is PKI (Public Key Infrastructure) using digital certificates.

In a previous article on how VPNs work, we looked at the importance of PKI from a high level. This article will give telecom managers, network planners and engineers a more detailed look at how PKI works in a VPN environment.

Public Key Infrastructure Defined

Public Key Infrastructure is the use of two digital keys mathematically related, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key. One of the keys is public, published to the world and the second is private, kept in a secure place. These keys can be used for authentication, encryption or digitally signing electronic data.

A simple Public Key Infrastructure starts with a Certificate Authority (CA), a software package operated in a high security area by a trusted party to issue X.509v3 digital certificates.

Digital Certificate. A digital certificate (cert) is an electronic data structure that binds the public key values to identifying information about the subject (carbon or silicon based life form) listed, and is digitally signed (authorized) by the issuing Certificate Authority. The cert assures any Relying Party (RP, party receiving the cert) using the public key that the associated private key is held by the correct remote subject (carbon or silicon based life form). Note: explanation of the fields of information in a cert can be found in RFC 2459(Internet X.509 Public Key Infrastructure Certificate and CRL profile) written in Jan. 1999.

In the high security area of the Certificate Authority there will also be an X.509v3 compatible database at a bare minimum. The CA operator issues the digital certificate to the End Entity (EE – IPSec endpoints in this case) and stores a copy of the cert in the database for future reference. The language used to query the X.509v3 database for any reason is Lightweight Data Access Protocol v3 (LDAP v3).

Handling of Invalid Certs

Even if a cert has not expired, it may be considered invalid or unusable for several reasons: the owner may no longer need it; it might have been compromised or stolen; the owner may have been issued a newer cert that takes precedence over the existing one.

In that case the CA operator may do one of two things. The cert may be listed on a CRL (Certificate Revocation List, X.509v2) and published at a given interval. The CRL stayed at v2 because it was agreed that there were no changes on it when the other components went to v3. Or the cert revocation is published using OCSP (Online Certificate Status Protocol) on an on-line server, which could be the X.509 v3 database server, providing that service.

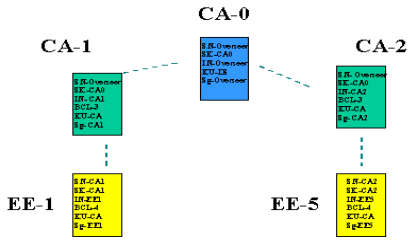
Each time an IPSec endpoint checks the validly of a cert presented to it for authentication, it checks its latest cached CRL or uses OCSP to see if that cert is listed. If it is listed, that means the cert is no longer valid, and the IPSec endpoint will reject it.

How a Complex PKI Works

A complex PKI can utilize multiple CAs with a Root CA. The Root CA holds a self-signed cert and issues certs to the subordinate CAs who in turn can issue certs to RAs (Registration Authorities) or LRAs (Local Registry Authorities). In operation the RA or LRA takes the initial request for a certificate from the requesting party and passes the authenticated request to its CA who issues the cert. The hierarchy of CAs resembles a tree, which is why the initial CA is identified as the Root CA (see illustration).

At this point a chain of trust has been established between all of the EEs (End Entities, in this case IPSec endpoints) from all of the subordinate CAs. But how does EE –1, the Relying Party (RP) whose cert was issued by CA-1, know that a cert EE – 5 issued by CA –

2 is trustworthy? Here are the steps showing how it works:



Complex PKI with a Root CA and multiple subordinate CAs.

1. EE – 1 first checks either the CRLs or uses OCSP to see if EE - 5 is a valid cert
2. EE – 1 then checks who signed the EE – 5 cert and finds that CA – 2 is the authorizing party
3. Now CA – 2 is an unknown to EE – 1 so it checks to see who signed cert CA – 2
4. EE-1 finds that it was CA – 0, the root cert who also signed cert CA – 1
5. CA-1 issued and signed the cert EE-1

This information proves the verification of EE – 5 because it is within the same PKI. This procedure is called "walking the chain of trust" or simply "walking the chain." These are the basic details of the operation of a single PKI. We will discuss multiple PKI implementations later in the article.

Certificate Policy Establishes Ground Rules

Whether they operate or outsource the CA, a company that implements a PKI should write a Certificate Policy (CP). The CP delineates the requirements for authentication to receive a certificate from the CA and also can indicate the level of authority (for example, "this cert allows signature authority for one million dollars").

In the case of an IPSec endpoint, the CP defines what information must be submitted to the CA for authentication prior to the issuance of a cert for that endpoint. It also details what information the individual cert will contain and how it will look. The CP will specify the CRL update or the requirements for posting the revoked cert notification to the OCSP server. The CP may also specify the physical security requirements that the CA must meet.

Assign and Register Your Object Identifier

When the CP is complete, it should be posted on the company's public web site. The company writing the CP should be registered with IANA (Internet Assigned Numbers Association) so that the CP can be assigned an OID (Object Identifier). An OID is the numeric representation of the company. That OID should be placed into the cert so that the RP (person receiving the cert) may able to find and read the CP of the cert by locating it on the identified company's web site. By reading the CP, the RP will be able to decide whether or not to rely on the cert.

Writing a Certificate Practice Statement

To successfully implement a CA, the operator of the CA must either write a specific Certificate Practice Statement (CPS) or provide a general CPS, depending on the level of authorization required. The CPS is an implementation document that supports the CP in detail, explaining how the CA meets the CP requirements. According to the American Bar Association, [ABA1], the CPS reference (OID) should be incorporated into the cert also. This information will then allow the RP to further verify the qualifications of the Certificate Authority.

Roll Your Own CA

If a company implements their own CA, they should create both the CP and the CPS. The best reference for writing a CP and CPS is RFC 2527 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework), written in March 1999. Prior to publishing the CP and CPS, the corporation's lawyers also should be consulted. However, do not expect assistance in the creation of either the CP or the CPS—unfortunately, there are only a few corporate lawyers who understand this field.

Although writing the CP and CPS might seem unnecessary because the company operating the CA has full control of their implementation, it is important for two reasons. First, it ensures optimal security, since the company has written documents for both operational guidance and security audit purposes. Second, it is needed if that company at some point wishes to cross certify with a

different PKI.

Cross certifying means that the cert issued by one PKI is usable in another PKI. Both the CP and CPS of each PKI will be reviewed by the other PKI to make sure that each other's certificates are "considered of equivalent value" in the required aspects (we can not say "are equal" because in the law that means exact wording). Cross certification is a simple physical operation—each CA issues the other a cert with a Policy Mappings Extension stating the above agreement. The difficulty is in reconciling the CP and CPS agreement between the two PKIs.

Cross Certification of PKIs can be cumbersome when there are multiple PKIs because the number of cross certificates expands geometrically. If there are two PKIs, there are two certs; however, with four PKIs, twelve certificates must be exchanged. At some point the individual EE no longer has the ability to walk the chain to ascertain the validity of a possibly legitimate certificate presented to it, i.e., the EE implementation does not have the computational ability to perform a chain walk of that duration. The solution to this is called a Bridged PKI.

A single Bridge CA exchanges cross certificates with the Root CAs of all of the PKIs. This reduces the length of the chain that an EE must follow to authenticate a certificate presented to it from out side of its PKI. This is the primary reason for a Bridged PKI, but it is also beneficial because it simplifies the nullification of a cross certification. Instead of having to post 12 certs to the CRL, only one has to be posted—the one issued by the Bridge CA in the cross certification.

We have discussed the majority of individual pieces that make a PKI work. Now comes the hard part.

Implementing PKI—Outsource or In-house?

There are two methods of implementing a PKI, one is to contract for the service and the other is to implement the operation in house. The decision of whether to outsource the service or implement it in-house must be made not only by comparing costs (which is roughly equal in the long term) but most importantly by considering the implementing company's overall security policy and its requirements. Does the company retain full control of its PKI, or does the company let someone else control that aspect of its security?

Although neither way is inexpensive, many companies, lacking sufficient knowledge of security principles, firewalls, and network topologies, find that contracting the implementation is easier. Specialized network engineering firms with trained resources can help set-up the network elements and recommend reputable CA firms to handle the PKI authentication process. In any case, a carefully thought-out PKI implementation can help ensure satisfactory operation of a VPN that assists the business with its goals.