Deploying Cisco IOS Security with a Public-Key Infrastructure

Using PKI Features in Cisco IOS Software Release 12.2T

Includes Release 12.2(8)T Enhancements

Introduction

Businesses can simplify some of the deployment and management issues that are encountered with secured data communications by employing a Public-Key Infrastructure (PKI) for management of encryption keys and identity. As businesses move more security-sensitive communications to the public Internet, an effective mechanism must be implemented to protect sensitive information from the growing criminal threat presented on the Internet.

There are three primary security vulnerabilities of communications over a publicly accessible network:

- *Identity theft*: intruder gains illegitimate access by posing as an individual who actually can access secured resources.
- *Eavesdropping*: intruder "sniffs" the data transmission between two parties during communications over a public medium.
- *Man-in-the-Middle*: intruder interrupts a dialogue and modifies the data between the two parties. The intruder would take over the entire session in an extreme case.

PKI reduces the likelihood that the secured communications channel is safe from an intruder posing as a trusted entity in the communications, or by knowledge of encryption keys falling into the wrong hands.

This document will focus primarily on the implementation of Cisco IOS IPsec networks that use PKI to manage encryption keys and end-host/end-user identity. Cisco IOS PKI is not limited to IPsec; therefore, the document will detail other technologies that may be augmented with PKI. This guide may be applied to a network of any size, which is composed of more than a handful of devices. Benefits of employing PKI for identity and key management increase with the number of encryption peers. This document will briefly discuss fundamental PKI technology concepts, but if a detailed discussion of PKI concepts is required, please see the "Additional Reading" section at the end of this document.

Benefits of PKI Deployment

- Simplified management of the security infrastructure through automation
- Increased security through difficulty of compromising certificate-based security
- Improved management integration for all secured services
- Tighter control of secure access to business resources

About PKI

PKI provides a hierarchical framework for managing the digital security attributes of entities that will engage in secured communications. In addition to human users, the following entities also participate in the PKI: encryption gateways, secure web servers, and other resources that require close control of identity and encryption.

Each PKI participant holds a digital certificate that has been issued by a Certificate Authority (CA). The certificate contains a number of attributes that will be used when parties negotiate a secure connection. These attributes must include the certificate validity period, end-host identity information, encryption keys that will be used for secure communications, and the signature of the issuing Certificate Authority. Optional attributes may be included, depending on the requirements and capability of the PKI.

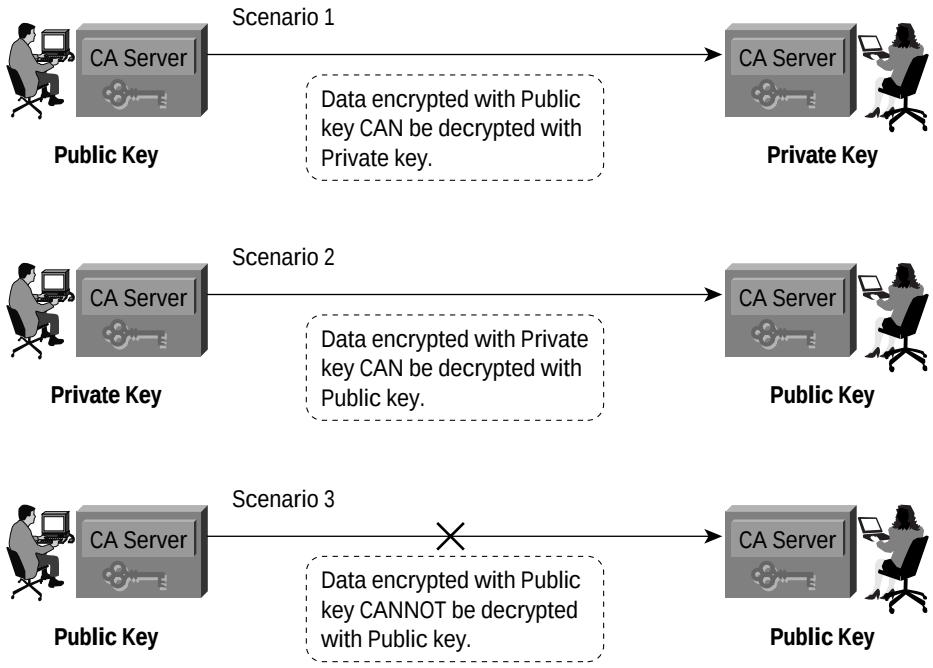
Public-Key Cryptography and Asymmetric Encryption

In asymmetric encryption, two different keys are used to render data illegible to anyone who may be eavesdropping on a conversation. The certificates contain the two components of asymmetric encryption: *public key* and *private key*.

Refer to Figure 1 for an illustration of the usage of public/private key pair in asymmetric cryptography. Data that is encrypted with the public key can be decrypted with the private key, and vice versa (Scenarios 1 and 2). However, data encrypted with the public key cannot be decrypted with the public key (Scenario 3). The parties who need to encrypt their communications will exchange their public keys (contained in the certificate), but will not disclose their private keys. The sending party will use the public key of the receiving party to encrypt message data and forward the ciphertext (encrypted data) to the other party. The receiving party will then decrypt the ciphertext with their private key.

Data encrypted with the public key cannot be decrypted with the public key. This prevents someone from compromising the ciphertext after acquiring both public keys by eavesdropping on the certificate exchange.

Figure 1. Usage of keys in asymmetric cryptography



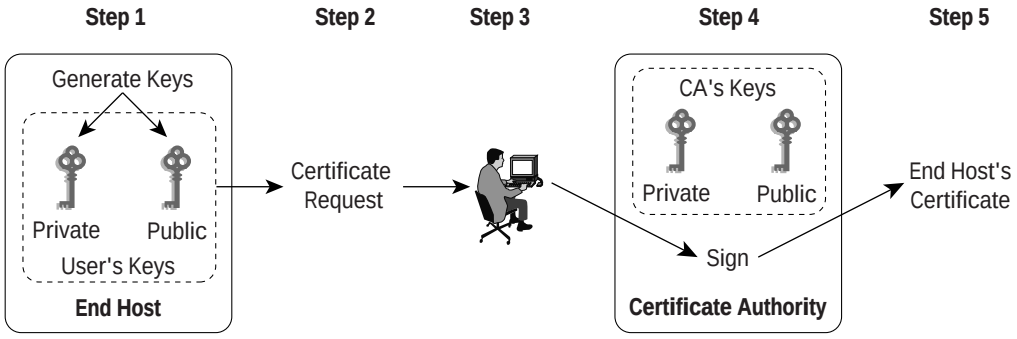
Enrolling in a Certificate Authority

Enrollment is the process of obtaining a certificate. It occurs between the end host desiring the certificate and the authority in the PKI that is responsible for providing certificates. The end hosts that will participate in a PKI must obtain a certificate, which they will present to the parties with whom they communicate when they need a secured communications channel.

The enrollment process for an end host (Figure 2):

1. End host generates a private-public key pair.
2. End host generates a certificate request, which it forwards to the CA or RA.
3. Manual, human intervention is required to approve the enrollment request, which is received by CA or RA.
4. After the CA or RA operator approves the request, the CA or RA signs the certificate request with its private key and returns the completed certificate to the end host.
5. End host writes certificate into a non-volatile storage area: PC hard disk or NVRAM on Cisco routers.

Figure 2. Certification Authority Enrollment Procedure



Simple Certificate Enrollment Protocol

Cisco IOS Software uses Simple Certificate Enrollment Protocol (SCEP) to communicate with a PKI. Cisco Systems developed SCEP to extend the capability of the certificate enrollment protocol that was developed by Verisign, Inc for Cisco. SCEP has achieved broad acceptance with the majority of Certification Authority software manufacturers, and Cisco competitors frequently implement protocols for certificate enrollment on their own VPN products.

SCEP offers a mechanism to support the secure transportation of key information and certificates between the different components of a PKI. Operations supported by SCEP include:

- CA/RA Public Key Distribution
- Certificate Enrollment
- Certificate Revocation
- Certificate Query
- CRL Query

SCEP employs the HTTP transport. Therefore, there is no requirement to implement support for new protocols on existing networks in the event firewalls must be configured to permit access to services on protected networks.

The end hosts employ a standard format for transportation of certificates and key information when they communicate internally and with the CA/RA. The fifteen Public Key Cryptography Standards (PKCS) define these. RSA Laboratories, a leading authority in development and maintenance of public key cryptography technology, publishes the PKCS documentation. The two Standards that are applied with SCEP are PKCS #7 (Cryptographic Message Syntax Standard) and PKCS #10 (Certification Request Syntax Standard).

CA/RA public key distribution is performed as clear-text HTTP transfers, as the end entity holds non-cryptographic key information from the CA or RA. After the end host receives the certificate, its fingerprint is compared against the fingerprint known at the CA or RA. This comparison is generally performed out-of-band, via email or phone conversation between the remote user enrolling the end host and the operator at the CA/RA console.

The end host may be *enrolled* via SCEP after retrieving the public key from the CA / RA. The enrollment request consists of a PKCS #10-formatted certificate request that is transmitted to the CA/RA in a PKCS #7 package. The certificate request will also include a Challenge Password and a request to include additional information in the certificate that the CA will return. The end-host operator/administrator should know the Challenge Password, which

is provided as an out-of-band authentication method for certificate issuance and verification activities. It will be made available to the CA/RA operator after the CA/RA receives the certificate request. As the end host generates the certificate request, the CA/RA's public key signs it.

The CA/RA decrypts the certificate request with its private key, and either:

1. Automatically signs the certificate request with its private key and returns the certificate to the end host, or
2. Waits until the CA/RA operator verifies the cert request with the end host operator and approves the request, after which the CA/RA signs the request and returns the cert to the end host.

SCEP supports *Certificate Revocation* by an out-of-band dialog between the end-host operator and the CA/RA operator. In the event the end host's keys are compromised, or if circumstances render the certificate invalid, the end host's operator will contact the CA/RA operator and present the Challenge Password. This is known at the end host and the CA/RA, because it was sent with the Enrollment Request. After the Challenge Password is verified, the CA/RA operator will follow the procedure for the given CA to revoke the end-host's certificate, and the revoked certificate will be published to the Certificate Revocation List.

If the end host does not have adequate memory to store its certificate, it may use the *Certificate Query* capability of SCEP to retrieve its cert from the CA. Alternatively, the certificate query may be completed via LDAP. In either case, the end host must know the serial number of the certificate and the Fully Qualified Domain Name used in the Certificate Enrollment Request.

The last functionality that SCEP supports is *CRL Checking*. When an end host is presented with a certificate, it will extract the URL for the CRL Distribution Point from the certificate, and try to check if the presented certificate is listed on the Certificate Revocation list. With Cisco IOS Software, SCEP is the lowest of three preferences for CRL checking protocol. HTTP is the most highly preferred option, followed by LDAP.

Certificate Authority versus Registration Authority

As PKIs are hierarchical in nature, the issuing certificate authority may be a root CA (the top-level CA in the hierarchy), or a subordinate CA. The PKI might employ additional hosts, called Registration Authorities (RA) to accept requests for enrollment in the PKI. RAs are employed to reduce the burden on CAs in an environment that supports a large number of certificate transactions, or where the CA is offline.

The Certificate Authority (aka: Certification Authority) is the central point of "trust" within the PKI. The end hosts in the organization trust the CA as the decisive source of information for the authenticity of other end hosts in the CA. When the CA issues a certificate, its digital signature on the certificate is a definitive mark that the end host, which holds the certificate, is part of the PKI.

In a more complex environment, the RA might be tasked with verifying user identity, establishing passwords for certificate management transactions, submitting enrollment requests (along with appropriate organizational attributes or other information) to the CA, and handling assorted tasks (ie: certificate revocation and re-enrollment).

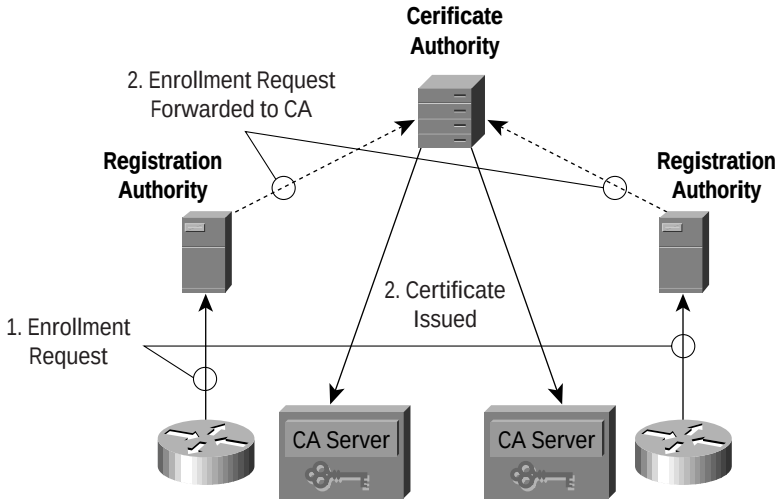
The RA only has the power to accept registration requests and forward them to the CA. It is not allowed to issue certificates or publish CRLs. The CA is responsible for these functions. As illustrated in Figure 3:

Step 1. End hosts will submit certificate requests to the RA

Step 2. After the Registration Authority adds specific information to the certificate request and the request is approved under the organization's policy, it is forwarded on to the Certification Authority

Step 3. The CA will sign the certificate request and send it back to the end host

Figure 3. CA/RA Relationship



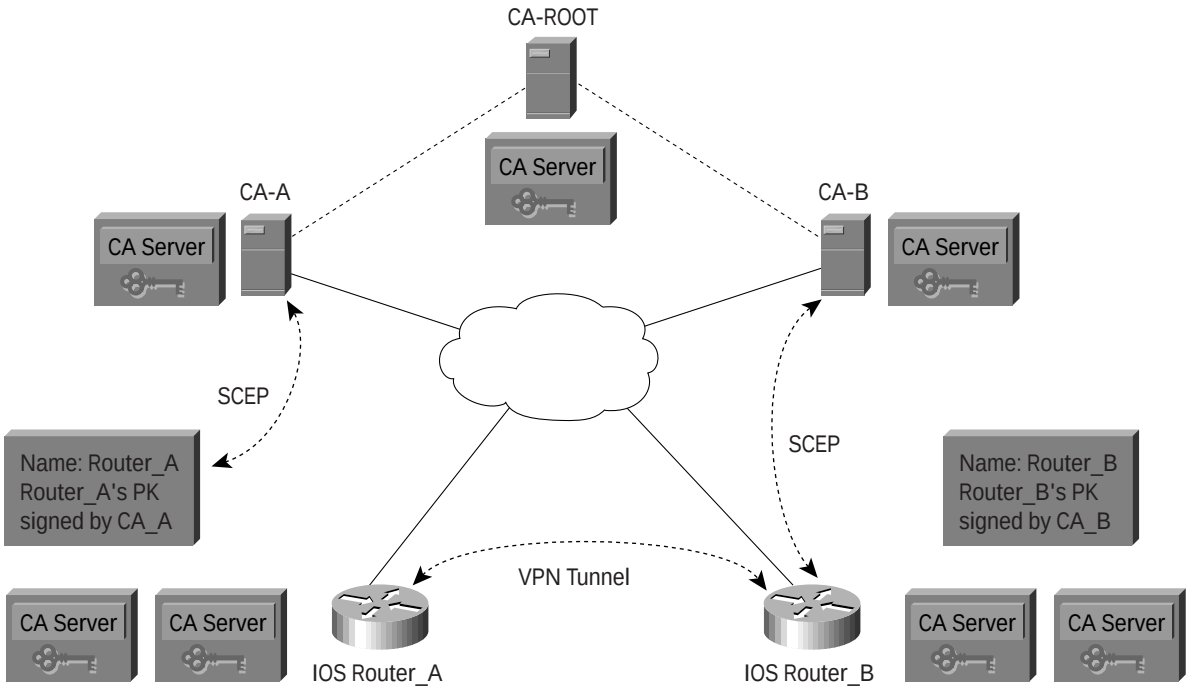
PKI Structure

The simplest PKI consists of one CA that integrates registration functionality and an LDAP server to serve as the CRL Distribution Point (CDP). A PKI of this simple nature will not scale effectively, offers little fault tolerance, and would be difficult to manage for a large organization with multiple, autonomous business units. These types of issues may be addressed by distributing components of the PKI to various parts of the organization along functional or geographic boundaries.

Figure 4 illustrates the structure of a large organization with distributed PKI resources. A large enterprise that has distant offices and the need for granular control over identity and security in different parts of the organization might deploy a PKI consisting of multiple CAs and RAs. In this situation, an end host (ie: Router A) will enroll with the CA (CA_A) that belongs to their part of the organization. When negotiating with Cisco IOS Router_B, which is enrolled in a different CA (CA_B, part of the same PKI), the end hosts will determine whether the CA with which the respective hosts are enrolled signs the certificates from its peers. If not, the end hosts will climb up the hierarchy of CAs until locating a CA that is common to both branches of the PKI. In this instance, CA_ROOT is the appropriate CA.

Cisco IOS Software currently supports only two levels of hierarchy in the PKI; however, additional levels will be supported shortly.

Figure 4. PKI Hierarchy and Certificate Chaining



Certificate Validation

After participating PKI entities have enrolled, they are ready to negotiate secure connections with each other.

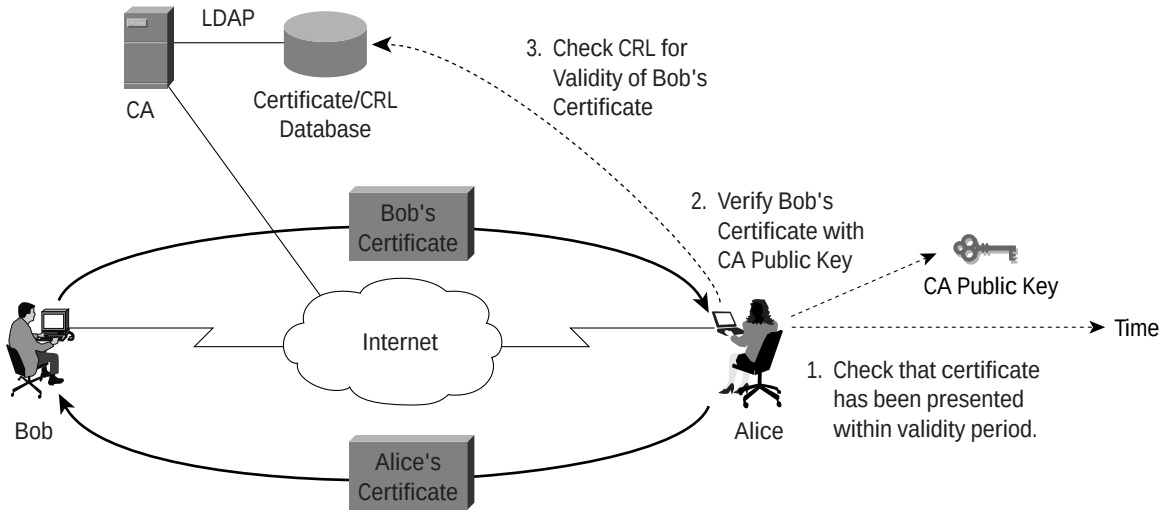
In most cases, two parties will initially contact one other via an application process, such as ISAKMP for an IPsec negotiation or HTTP for an SSL negotiation. The end hosts will eventually exchange their certificates for mutual verification.

Figure 5 illustrates the steps during a certificate validation between two parties, Alice and Bob. The parties examine the certificates to determine if

- The cert is being presented within its validity period
- The CA that signed the cert is a component of the appropriate PKI
- The certificate is on a revocation list

If the certificate passes all the validity criteria, the parties will use the public keys contained within the certificates to negotiate the IPsec Security Associations (SA). All data to be transmitted through the SA will be encrypted by the peers' public keys, and will be decrypted by the receiving party, using the peer's private key. IPsec SAs are generally set with a re-key interval, which will cause a renegotiation of the keys used on the SA after the SA encrypts a certain amount of data, or a specific time interval passes, whichever comes first. When renegotiation occurs, the cryptographic components of Cisco IOS Software will ask that the peer's certificate be re-transmitted, and will request that the verification process be repeated.

Figure 5. Certificate Verification



PKI Components Required for Deployment

There are simple requirement associated with the deployment of an IPsec VPN with PKI. There are multiple solutions available to address the needs for the various components.

One a CS is required for the simplest option. This involves signing up with an online CA vendor to provide certificates. Participating PKI entities (network devices, human users employing application software, etc) will require software components to interoperate with the PKI. PKI components are embedded in the VPN software in the case of IPsec VPNs. Other PKI-enabled applications include web browsers, wireless connectivity components, and email software.

Subordinate CAs may be deployed throughout the organization if a more advanced PKI is required; however, PKI design is outside the scope of this document. Routers and clients can be enrolled when the PKI is in place, or they may be pre-configured to auto-enroll upon deployment.

The CRL is another crucial PKI component. This is a list of certificates that were formerly valid within the PKI, but have been revoked for any reason. These reasons could include any of the following:

- Compromise of keys within certificate
- Loss of access privileges for user/device
- Change of PKI structure requiring cert re-issue

Certificates issued for a given PKI contain CDP location, the CRL Distribution Point. During certificate verification, the verifying user will attempt to gain access to the CRL at the location indicated within the certificate. The CDP may appear as a URL, depending on the publishing method. The supported publishing mechanisms in Cisco IOS Software are HTTP, LDAP, and SCEP (listed in order of preference).

The anticipated size of the CRL may substantially impact PKI design, as revoked certificate lists can be lengthy, particularly in environments with large numbers of users or high rates of certificate turnover. Some CAs place limits on the maximum size of CRLs, so the PKI designer should consult the CAs documentation for information about the particular CA. CRLs can be implemented with a great deal of flexibility in their granularity, which accommodates varying requirements for cert revocation procedure.

Design Considerations and Planning

Upon initial design, designers must consider what functionality will be demanded from the PKI.

Organizations that support complicated PKIs prefer to keep the root CA offline. While this reduces vulnerability to electronic attacks, it also means that additional PKI components must be deployed. This may consist of subordinate CAs or Registration Authorities (RAs). This ensures that access to the PKI is available for initial enrollment, re-enrollment, certificate status checking, and other tasks. At some point, the subordinate devices will be enrolled in the root CA, to associate them with the PKI. After they are enrolled in the root CA, they have the authority to process certificate enrollment requests, certificate revocation, and other cert management tasks.

As certificates are revoked, they are published in the CRL, which is generally available from LDAP or other services, depending on the CA capability. The CA signs the CRL, and a validity date period is embedded in the CRL. A shorter period should be set for CRL expiration in an environment where:

- There will be a significant amount of cert revocation or
- It is critical that security peers in the PKI are aware of cert revocation activity.

All PKI-participating peers should be able to access the CRL. The default behavior of Cisco IOS Software is to retrieve the certificate's CRL from the Certificate Distribution Point location, which is embedded in the presented cert. Once a router retrieves the CRL, it keeps the CRL in its cache until the CRL reaches the expiration date/time. The router will retrieve the CRL again when the cert linked with the CRL is presented. The router may have several CRLs in its cache simultaneously, depending on CRL granularity. While CRL checking is enabled by default, it can be disabled if certificate status is not an issue. Of course, CRL checking should be enabled when the network requires a high degree of security.

Another component of the validation of a certificate presented for security negotiation is the verification of the certificate's validity period. This leads to the next topic for a successful PKI implementation: the requirement for provision of accurate time to remote devices.

PKI and Accurate Time

An accurate time source must be available in order to enroll a cryptographic device in a PKI, and to check certificate validity from negotiating peers.

When crypto peers present their certificate to each other, the validity date is amongst first things that will be checked within the cert. Cisco IOS Software will compare the beginning and end of the certificate's validity period (embedded in the certificate), to the time and date in the router's clock. If the router's current date is within the certificate's validity period, the router goes on to check the validity of other components of the certificate. The router must have access to the correct time, either through manual configuration of the system clock, accurate time sources (ie: NTP), or clock adjustment via SNMP.

High-end Cisco routers (ie: Cisco 7100 and 7200 Series Routers), which will commonly be deployed for higher-scale hub sites, have a hardware clock. This can store the time across reboots. If NTP is employed at the hub site, the NTP server must be accessible via a trustworthy connection; this prevents an intruder from gaining access with an out-of-date cert by falsifying the time information being presented to the router.

Nearly all Cisco IOS Software VPN remote sites, such as branch offices and home users, use products from the Cisco Systems access router family for communications security. Many of these routers (ie: Cisco 800, 900, 1700, 2600, 3600, and 3700 Series Routers) have no internal hardware clock, which would maintain the clock through a reboot. After an access router is rebooted, it reverts back to a time set by the firmware, rather than the current time. This is an undesirable condition, as the default time on a router is most likely earlier than the beginning of the device's certificate's validity period. Likewise, it is earlier than the validity period of the certificates that the device's peers will be presenting.

There are currently two options for configuring the "good" time on these Access Router platforms: set the clock manually, or retrieve the time via Network Time Protocol (NTP). As described earlier, trustworthy access to time servers is crucial.

Conversely, this is not quite as important at remote site, which will not generally require the same degree of protection for sensitive resources as might be required at a central site.

An illustration of a simple central-site security model is given in the forthcoming section: "Lab System Configuration".

Configuring Cisco IOS Software Support for PKI

Cisco IOS Software must be correctly configured, in order to interoperate effectively with a PKI.

The following section illustrates a sample configuration entry checklist. This indicates the basic values for configuring a Cisco router to participate in a PKI. It labels the configuration entries just as they will be configured on a router.

To understand the various keywords and their relationships with the actual components of the PKI, a short definition is in order for all the various configuration keywords.

- *Enrollment URL*: The router must contact the CA/RA, in order to enroll in the PKI. Cisco IOS Software will enroll with the CA via SCEP, which uses HTML as the application protocol. This explains why the router must have a URL to enroll. The CA documentation should offer the enrollment URL, which varies from vendor to vendor.
- *Enrollment Interface*: By default, the router will originate the enrollment request from the same interface that transmits the request. If a different interface's address should be included in the enrollment, select the IP address or interface that will be used.
- *Router's FQDN*: FQDN will only be configured if it will vary from the host and domain name offered in the Cisco IOS Software configuration. If additional x.500 attributes need to be offered at enrollment time, they must be written in the config and handed to the RA/CA at enrollment time.
- *CRL Query Location*: The router will retrieve the CRL via LDAP. The URL of the LDAP server must be provided, so the router can find the CRL resources.
- *CRL Requirement*: This will be further explained in the "Trustpoint CLI" discussion. Maintain the default setting of the router if CRL checking is critical. If certificate revocation status is not required, select "best effort" or "optional" after reading the description of these modes in the "Trustpoint CLI" discussion.

Configuration Worksheet

Enrollment URL:_____

Enrollment Interface:_____

Router's FQDN:_____

CRL Query Location:_____

CRL Requirement: ____Required ____Best Effort ____Optional

Enrollment Mode: ____Auto ____Manual

PKI Support In Cisco IOS Software

Cisco IOS Software began to support a limited set of PKI features in Cisco IOS Software Release 12.0. As interest in PKI has grown for securing IPsec VPNs, a number of features have been incorporated to make PKI more useful with Cisco IOS VPNs, particularly in Release 12.2T.

Recently released features include:

- Trustpoint CLI/Certificate Management Interface enhancements
- Certificate Auto-enrollment
- Distinguished Name-based crypto maps
- Support for multiple key pairs

Cisco IOS Software Release 12.2T supports multiple features that are useful for integrating a PKI with IPsec VPNs.

Before features can be discussed, it is necessary to include a brief description of Cisco IOS Software configuration for interoperability with a Certificate Authority.

The earliest CA interoperability commands, which are part of Cisco IOS Software Release 12.0, contain the following config syntax:

```
crypto ca identity domain.com
 enrollment url http://ca_server
 query url ldap://ca_server
```

This configuration presents the hostname of the CA server and the location of enrollment and CRL checking. Very few options were configurable, and the feature set had limited applicability. As PKI started to become a more widely requested option, the need for new features was realized and Cisco IOS Software introduced several improvements to the certificate management interface:

Trustpoint CLI

This feature appeared first in Cisco IOS Software Release12.2(8)T

The trustpoint CLI combines and replaces the earlier crypto ca identity and crypto ca trusted-root commands. This creates a unified set of commands for the configuration of all PKI options, rather than multiple command sets with differing capabilities. Trustpoint CLI also offers multiple new commands for configuring attributes that will be passed to the CA.

The password keyword writes a revocation password into the router's configuration, so that a prompt will not be displayed when the router is enrolled. An encrypted form of the password will be stored in the router's configuration.

The ip-address keyword specifies an IP address to include in the certificate. The default for manual enrollment prompts the user for this information. The default for auto-enroll is to not include an IP address in the certificate request. Either an interface name or an IP address may be specified with the ip-address keyword.

The serial-number keyword configures inclusion of the router's serial number in the certificate enrollment request. If the serial-number keyword is present, the enrollment request will automatically include the router's serial number. If no serial number in the enrollment request is desired, configure serial-number none. If no serial number setting is configured, a prompt will be raised at enrollment time.

The subject-name command allows the entry of x.500-compatible name attributes. The default behavior is for the Fully Qualified Domain Name that is assembled from the hostname and domain name to be included in the cert enrollment request in addition to the name specified in subject-name.

When routers are enrolled in a PKI, "IKE" is the default usage included in the cert request. If different usage parameters are desired for the certificate request, the usage keyword specifies the new value.

A new option for CRL checking has been added. In the past, there were two options: CRL checking could be enabled by default, or it could be completely bypassed with the crl optional command. A new switch is available, the crl best-effort command. If the CRL is available, the router will check and cache the CRL. If the CRL is unreachable, the router will process the cert without the CRL. Every time a certificate is presented, if crl best-effort is configured, the router will attempt to reach and check the CRL.

Auto Enrollment

This feature appeared first in Cisco IOS Software Release 12.2(8)T.

The auto-enrollment feature is an enhancement targeted to ease the management of certificates on routers. It eliminates manual intervention when a Cisco IOS device is enrolled or re-enrolled with a CA. If routers are manually enrolled in a PKI when they are deployed, they must be connected to the network; console or telnet access to the device must be available to issue commands, in order to enroll the devices. Configuration access to devices can be difficult, as routers may be deployed to home-user or branch office locations that do not have skilled personnel available to handle enrollment tasks. Furthermore, all certificates have a finite lifespan; when expired, they will not offer valid credentials when presented to a crypto peer when a device attempts to initiate a secured connection. To resolve the problem of the expired certificate, a device must be re-enrolled with the PKI. Once again, this presents the requirements of skilled personnel who can access the configuration interface on the device and re-enroll it.

Auto-enrollment addresses these issues by checking the device's enrollment status when availability of the cryptographic connection is required. If the router is not enrolled, or if the certificate that the router is holding is near its expiration date, it will automatically contact the configured RA to enroll or renew its certificate. This simplifies deployment of remote-site routers by allowing pre-configuration before shipment to branch office or home office users, and reduces the administrator workload maintaining certificates as they expire.

Configuration is quite simple, requiring the addition of only one line to the trustpoint config:

```
crypto ca trustpoint sanjose
 enrollment mode ra
 enrollment url http://sj-ca1.cisco.com/
 crl query ldap://sj-ca1.cisco.com/
 auto-enroll
```

When a router is deployed, it needs the CA cert prior to auto-enrollment (this applies when the auto-enroll feature is enabled). The CA cert can be installed via SCEP or TFTP, as per the trustpoint CLI discussion.

Once the router is set up with the trustpoint configuration and the CA cert has been installed, the config will be written, and the device may be deployed to where it will be installed in the network. Auto-enroll will update the router's cert any time it is expired or if has not yet been installed, but it will not renew a revoked cert. The router will write the newly retrieved certificate (and keypair, if applicable) to NVRAM, unless the router is in configuration mode with a user session on the console or a telnet session. If the router is in config mode, the user must manually write the new certificate to memory. This prevents saving temporary config changes unintentionally. In that case, an informational message will appear , and the new cert (and keypair, if applicable) will be saved when the operator issues a write memory command.

Auto-enroll can also regenerate the keypair associated with re-enrollment of the cert. If the specified key does not exist, or if the optional parameter regenerate is given to the auto-enroll command, a new keypair will be generated.. The rsakeypair subcommand will specify the name and size(s).

Distinguished Name-Based Crypto Maps

This feature appeared first in Cisco IOS Software Release 12.2(4)T.

Earlier releases of Cisco IOS Software included PKI functionality, and were somewhat limited in their capability to offer different cryptographic policies to negotiated peers. Different crypto map configurations may be required, based on the specific connection. These might be particularly different in terms of defining different tunnel policies by access list, varying requirements for encryption strength, sensitivity for key lifetime duration, and other factors affecting the IPsec Security Associations that are configured by the crypto map.

DN-based crypto maps offer a solution to this earlier limitation by negotiating different crypto policies with peers, based on the distinguished name fields contained in the peer certificate. When a peer offers its certificate, a router examines the certificate for the Distinguished Name field and compares it to the list of configured crypto maps. When there is a match between the DN attributes in the certificate and the attributes specified in the identity label, the crypto negotiation proceeds, according to the parameters specified in the associated crypto map.

The router's crypto map configurations includes naming an identity label in the crypto map, and the configuration of the identity label where DN components are identified:

```
crypto map mymap 1 ipsec-isakmp
 set peer 172.16.172.10
 set transform-set mytransform
! call out identity for crypto map
 set identity chicagovpn
 match address 102
! define identity values
crypto identity chicagovpn
! the following are included as examples
 dn OU=Chicago
! “dn O=xxx” and “dn OU=xxx” can and will be seen together
 dn O=Cisco
! “fqdn xxx” will not be seen in an identity with “dn O=”
! or “dn OU=”, they are mutually exclusive.
 fqdn chicago.cisco.com
```

Support For Multiple Key Pairs Per IOS Router

This feature first appeared in Cisco IOS Software Release 12.2(8)T.

Prior to the implementation of this feature, a router could only offer one set of keys to a CA at enrollment time. If a router were enrolled in multiple CAs with different key policies, Cisco IOS Software could not meet these requirements. With the addition of support for generation and storage of multiple key pairs, a router can now carry more than one pair of RSA keys and associate them with a trustpoint profile.

```
crypto key generate rsa general-purpose exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url http://examplecakeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

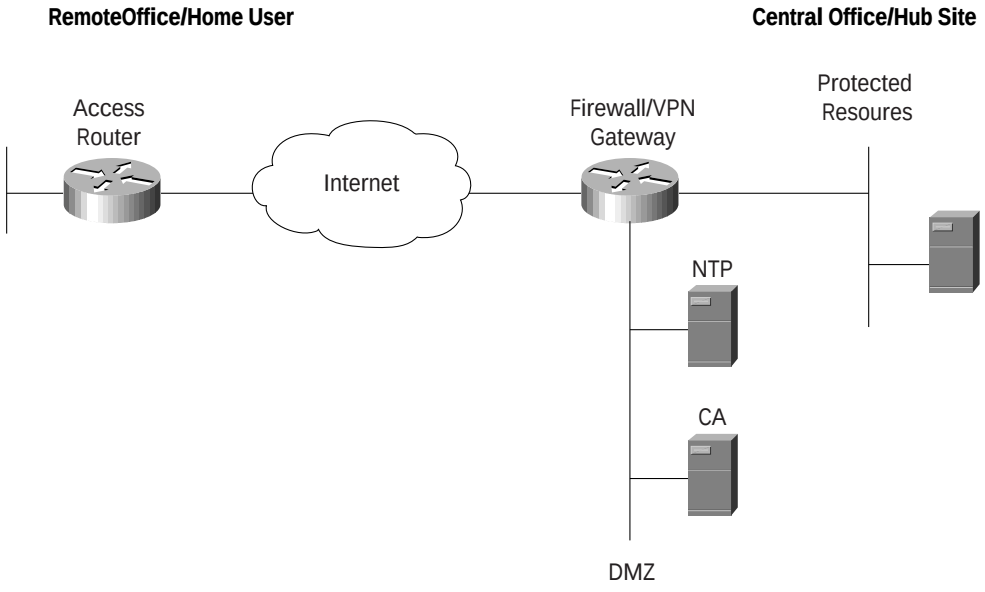
Lab System Configuration

A simple network can provide an overview of Cisco IOS VPN functionality with PKI. Tests can easily be conducted on cert-based authentication for IPsec VPNs that have a pair of routers for site-to-site tunnels, as well as the Cisco VPN client to be used for remote access. A CA will be needed to provide certificates for the VPN peers (the routers and the client). It must be accessible from the public network, across which peers will communicate . It does not matter if the CA is hosted somewhere else on the public network, or if it is connected to the private network by one of the IPsec peers. The appropriate protocols must be allowed to pass to the CA; specifically, HTTP for enrollment and LDAP for CRL checking.

In the configuration examples, the hub-site router configuration will contain the IPsec crypto maps, crypto trustpoint configuration, and a simple set of firewall rules to allow access to a DMZ, where RA will be deployed.

As per the earlier discussion about trustworthy time access, the NTP server that provides time for the CA, hub site router, and all remote sites is also connected to a DMZ where the CA resides. Along with all other firewall rules that will be governing access to the DMZ, NTP access will be provided to the public.

Figure 6. Lab Net



- Green-colored network segments: private network space, numbered in 172.16.x.x networks. Traffic in this area will not be protected by encryption.
- Yellow network segment: Internet-accessible space in DMZ, protected by sufficient firewall policy to allow http, ldap, and ntp requests from the public Internet.
- Red network segments: public network domain, where traffic will be protected by encryption. Red and yellow segments are in 192.168.x.x networks, presumed routable for this exercise.

Both of the routers participating in the secured network (Access Router and Firewall/VPN Gateway devices) are running Cisco IOS Software Release 12.2(8)T:

Firewall/VPN Gateway:

```
itd-7206-l#sh ver
Cisco IOS Software
IOS (tm) 7200 Software (C7200-JK9O3S-M), Version 12.2(8)T5, RELEASE SOFTWARE (fc1)
```

Access Router:

```
itd-1720-l-b#sh ver
Cisco IOS Software
IOS (tm) C1700 Software (C1700-K9O3SY7-M), Version 12.2(8)T5, RELEASE SOFTWARE (fc1)
```

Two sets of configuration files are illustrated, one set for manual enrollment of the IPsec peers to a CA, and one set for automatic enrollment of the peers to the CA.

Manual Enrollment Scenario

The following config and debug output illustrates console activity on access router indicated in the lab network diagram.

```
Current configuration : 9465 bytes
!
! Last configuration change at 16:30:01 MDT Mon Jul 22 2002
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname itd-1720-l-b
!
!
username cisco password 0 cisco
memory-size iomem 20
clock timezone MST -7
clock summer-time MDT recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip domain-name cisco
ip host rockies 192.168.1.20
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint rockies
 enrollment mode ra
 enrollment url http://rockies:80/certsrv/mscep/mscep.dll
 crl query ldap://rockies
 crl best-effort
crypto ca certificate chain rockies
 certificate 61B45549000000000017
 30820339 308202E3 A0030201 …
! bulk of cert removed…
 …F38F9CF5 F0DEFDA3 4B2E451E 54
 quit
 certificate ra-sign 61021B04000000000004
 308203A6 30820350 A0030201 …
! bulk of cert removed…
 …040A1CBA B59099A2 CA4B
 quit
 certificate ra-encrypt 61021CC7000000000005
 308203A6 30820350 A0030201 …
! bulk of cert removed…
 …65074835 1DE93DD6 2635
 quit
 certificate ca 749017C5EB96B39C4D61B607A71C5F1B
```

```
 30820256 30820200 A0030201 …
! bulk of cert removed…
 …6FE04108 328A8FFB D3123A9B 5105
 quit
!
crypto isakmp policy 1
crypto isakmp identity hostname
!
!
crypto ipsec transform-set sha-des esp-des esp-sha-hmac
!
crypto map encrypt 1 ipsec-isakmp
 set peer 192.168.101.2
 set transform-set sha-des
 match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.103.2 255.255.255.0
 half-duplex
 crypto map encrypt
!
interface FastEthernet0
 ip address 172.16.103.1 255.255.255.0
 no keepalive
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.103.1
ip route 172.16.0.0 255.255.0.0 192.168.103.1
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 172.16.103.0 0.0.0.255 172.16.0.0 0.0.255.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
line vty 5 15
 login
!
no scheduler allocate
ntp clock-period 17180039
ntp server 192.168.1.2
end
```

Manual Enrollment Key Generation, CA Authentication and Enrollment

```
itd-1720-l-b#conf t
Enter configuration commands, one per line. End with CNTL/Z.
itd-1720-l-b(config)#crypto key generate rsa
The name for the keys will be: itd-1720-l-b.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: (enter)
% Generating 512 bit RSA keys ...[OK]

itd-1720-l-b(config)#
00:02:51: %SSH-5-ENABLED: SSH 1.5 has been enableditd-1720-l-b(config)#crypto ca auth
rockies
Certificate has the following attributes:
Fingerprint: 2DCEC066 FCABB674 BF81BFAF 76CD10FA
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
itd-1720-l-b(config)#crypto ca enroll rockies
%
% Start certificate enrollment ..

% The subject name in the certificate will be: itd-1720-l-b.cisco
% The serial number in the certificate will be: 7F2BA4B1
% Include an IP address in the subject name? [no]: (enter)
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

itd-1720-l-b(config)# Fingerprint: 261DD46D B43FB258 E69E58CA 991B03D1

00:03:31: CRYPTO_PKI: status = 102: certificate request pending
00:03:54: CRYPTO_PKI: status = 102: certificate request pending^Z
itd-1720-l-b#
00:04:02: %SYS-5-CONFIG_I: Configured from console by console
itd-1720-l-b#
00:04:56: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Auto-Enrollment Scenario

The auto-enrollment scenario uses the same lab network setup and configuration as the manual enrollment scenario; however, one line of configuration has been added for the trustpoint:

```
crypto ca trustpoint rockies
 enrollment mode ra
 enrollment url http://rockies:80/certsrv/mscep/mscep.dll
 crl query ldap://rockies
 crl best-effort
 auto-enroll
```

For the manual enrollment scenario, the router had to be manually enrolled with the CA during configuration. With the auto-enroll option configured, keys still need to be generated on the router, and it must authenticate the CA; however, enrollment is not required. When traffic that matches the encryption configuration is passed through the router, it will automatically enroll with the CA. The new certificate that the CA issues to the router is stored in RAM, but not written to NVRAM. *The write mem command must be issued so the router will store its certificate.*

Auto-Enrollment Key Generation and CA Authentication

```
itd-1720-l-b#conf t
Enter configuration commands, one per line. End with CNTL/Z.
itd-1720-l-b(config)#crypto key generate rsa
The name for the keys will be: itd-1720-l-b.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
 General Purpose Keys. Choosing a key modulus greater than 512 may take
 a few minutes.

How many bits in the modulus [512]: (enter)
% Generating 512 bit RSA keys ...[OK]

itd-1720-l-b(config)#
00:02:51: %SSH-5-ENABLED: SSH 1.5 has been enableditd-1720-l-b(config)#crypto ca auth
rockies
Certificate has the following attributes:
Fingerprint: 2DCEC066 FCABB674 BF81BFAF 76CD10FA
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
itd-1720-l-b(config)#
```

Auto-Enrollment System Testing

```
itd-1720-l-b#deb cry pk tra
Crypto PKI Trans debugging is on

itd-1720-l-b#ping
Protocol [ip]:
Target IP address: 172.16.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.103.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

itd-1720-l-b#% Time to Re-enroll trust_point rockies%
% Start certificate enrollment ..

% The subject name in the certificate will be: itd-1720-l-b.cisco
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.
 Fingerprint: 91D3732F DBB9FE66 FF099638 A36DB820

22:29:50: CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=rockies HTTP/1.0

22:29:50: CRYPTO_PKI: http connection opened
22:29:51: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 24 Jul 2002 19:24:09 GMT
Content-Length: 2525
Content-Type: application/x-x509-ca-ra-cert

Content-Type indicates we have received CA and RA certificates.

22:29:51: CRYPTO_PKI:crypto_process_ca_ra_cert()

22:29:51: CRYPTO_PKI: crypto_process_ra_certs() For:rockies
22:29:51: CRYPTO_PKI: transaction PKCSReq completed
22:29:51: CRYPTO_PKI: status:
22:29:51: CRYPTO_PKI: http connection opened
22:29:54: CRYPTO_PKI: received msg of 687 bytes

22:29:54: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 24 Jul 2002 19:24:12 GMT
```

```
Content-Length: 542
Content-Type: application/x-pki-message
22:29:54: CRYPTO_PKI: status = 102: certificate request pending
22:29:54: CRYPTO_PKI: http connection opened
22:30:16: CRYPTO_PKI: received msg of 687 bytes
22:30:16: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 24 Jul 2002 19:24:15 GMT
Content-Length: 542
Content-Type: application/x-pki-message

22:30:16: CRYPTO_PKI: status = 102: certificate request pending
22:30:26: CRYPTO_PKI: All sockets are closed.
22:30:36: CRYPTO_PKI: All sockets are closed.
22:30:46: CRYPTO_PKI: All sockets are closed.
22:30:56: CRYPTO_PKI: All sockets are closed.
22:31:06: CRYPTO_PKI: All sockets are closed.
22:31:16: CRYPTO_PKI: resend GetCertInitial, 1
22:31:16: CRYPTO_PKI: resend GetCertInitial for session: 0
22:31:16: CRYPTO_PKI: http connection opened

22:31:18: CRYPTO_PKI: received msg of 1824 bytes
22:31:18: CRYPTO_PKI: HTTP response header:
 HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 24 Jul 2002 19:25:37 GMT
Content-Length: 1678
Content-Type: application/x-pki-message
22:31:18: CRYPTO_PKI: status = 100: certificate is granted
22:31:19: CRYPTO_PKI: All enrollment requests completed.
22:31:19: CRYPTO_PKI: All enrollment requests completed.
22:31:19: %CRYPTO-6-CERTRET: Certificate received from Certificate Authority
22:31:19: CRYPTO_PKI: All enrollment requests completed.
22:31:19: %CRYPTO-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save
new certificate

22:31:29: CRYPTO_PKI: All enrollment requests completed.
```

Failure Diagnosis

In the event that devices do not appear to be properly enrolling to the CA, or if tunnels are not established due to authentication failure, Cisco IOS Software generates useful debug output if the correct debug settings are enabled. These debug and show commands may be broken into two subsets: debugging transactions with the certificate authority, and for monitoring IPsec tunnel establishment and status.

PKI debugging:

debug crypto pki transactions—Useful for troubleshooting CA enrollment, cert verification, and CRL checking. Debug ldap will not display any messages during CRL checking via ldap.

debug crypto pki messages—Verbose output detailing interaction between router and CA, displays actual dialog between parties. Unless byte-for-byte detail of dialog is needed, use debug crypto pki transactions.

sh crypto ca certificates—Displays information embedded in certificates regarding x.500 attributes, issuer, validity period, and CRL Distribution Point.

sh crypto ca crls—Displays summary of CRLs that are cached in a router. Information displayed includes CRL expiration, issuer, and location of CDP.

```
CRL Issuer Name:
 CN = BLDR-TME, O = ITD, L = Boulder, ST = CO, C = US
 LastUpdate: 14:41:11 MDT Jul 18 2002
 NextUpdate: 03:01:11 MDT Jul 26 2002
 Retrieved from CRL Distribution Point:
  http://rockies/CertEnroll/BLDR-TME.crl
```

sh crypto ca timers—Lists remaining validity time for various objects related to the PKI a device is enrolled with. CRLs, certificates, and trustpoint timers are included.

```
| 6d16:39:31.048
 | 6d16:39:31.048 CRL http://rockies/CertEnroll/BLDR-TME.crl
 |3797d18:44:32.076 RENEW rockies
```

sh crypto ca trustpoints—Displays trustpoint information. Lists CA name, DN attributes, and locations for enrollment and CRL.

```
Trustpoint rockies:
 Subject Name:
 CN = BLDR-TME
 O = ITD
 L = Boulder
 ST = CO
 C = US
 Serial Number: 749017C5EB96B39C4D61B607A71C5F1B
 Certificate configured.
 CEP URL: http://rockies
 CRL query url: ldap://rockies
```

show crypto key pubkey-chain rsa—Used to display

```
Codes: M - Manually configured, C - Extracted from certificate

Code Usage  IP-Address                                                  Name
C Signing                                                               X.500 DN name:
                                                                        CN = boulder
                                                                         O = cisco
                                                                         L = boulder
                                                                         ST = colorado
                                                                         C = US

C Encrypt                                                               X.500 DN name:
                                                                        CN = boulder
                                                                         O = cisco
                                                                         L = boulder
                                                                         ST = colorado
                                                                         C = US

C Signing                                                               X.500 DN name:
                                                                        CN = BLDR-TME
                                                                         O = ITD
                                                                         L = Boulder
                                                                         ST = CO
                                                                         C = US

C General                                                               itd-1720-l-b.cisco
```

Glossary

CA—Certificate Authority. A network service that is recognized as a trustworthy entity for establishing another entity's identity and linking that entity's encryption keys with its identity.

CDP—CRL Distribution Point. A location in a PKI where a particular certificate's CRL is available. CDP is embedded in a host's certificate, so a validating router can easily determine where to check a certificate's status.

CRL—Certificate Revocation List. A list of certificates that is no longer valid, due to revocation. The CRL is signed by the issuing CA and contains beginning and ending dates for its validity period.

Encryption peer—A device that will be the partner in an encrypted dialogue.

End host—PKI "users". End hosts are the components of a PKI that will enroll with the CA, and will obtain certificates to use in negotiating secure communications with other end hosts in the PKI.

IKE—A hybrid protocol that integrates the Oakley and Skeme key-exchange mechanisms within the ISAKMP protocol. IKE is used to negotiate authenticity and encryption on secure communications. Most commonly used for IPsec, IKE has application with other security protocols as well.

IPsec—A group of standards that define application of encryption and authentication mechanisms to IP traffic.

LDAP—Lightweight Directory Access Protocol. LDAP is a directory structure for storing information about the entities of an organization. The structure is defined by the x.500 standard.

Peer certificate—The certificate that an encryption peer presents during a security negotiation.

RA—Registration Authority. A secondary member of a PKI, which assists the CA in handling registration requests for the PKI. Used to offload enrollment and other cert management burdens from CA.

RSA Keys—A pair of keys generated for Rivest-Shamir-Adleman public-key cryptography. The key pair consists of a public and private key. In a PKI application, the end host generates the keys, and the public key will be forwarded to the CA for signature and incorporation in the encryption peer's digital certificate.

SCEP—Simple Certificate Enrollment Protocol. A protocol developed by Cisco to allow communication between a routers and CAs when requesting enrollment and other tasks in a PKI.

x.500—see LDAP

x.509—The mostly commonly-used standard for digital certificates. It defines certificate structure, handling, enrollment procedures, and most other facets of cert usage. The standard is currently in its third version, and very few organizations employ versions 1 and 2.

Additional Reading

Adams, Carlisle and Steve Lloyd, Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, 1999

IETF Public-Key Infrastructure Working Group:

http://www.ietf.org/html.charters/pkix-charter.html

Discussion of Simple Certificate Enrollment Protocol:

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm

RSA Public Key Cryptography Standards:

http://www.rsasecurity.com/rsalabs/pkcs/

References

RFC 2459—Internet X.509 Public Key Infrastructure Certificate and CRL Profile

RFC 2510—Internet X.509 Public Key Infrastructure Certificate Management Protocols

RFC 2511—Internet X.509 Certificate Request Message Format

RFC 2527—Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

RFC 2528—Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates

RFC 2559—Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2

RFC 2585—Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP

RFC 2587—Internet X.509 Public Key Infrastructure LDAPv2 Schema

CCO References

- Trustpoint CLI:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm
- Certificate Enrollment enhancements:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm
- Configuring crypto maps for DN-based access control:

  http://www.cisco.com/warp/public/471/vpn_dn.html - tools
- Multiple RSA Key Pair Support:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm - 42193

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe