



Cisco IOS PKI Overview: Understanding and Planning a PKI

First Published: May 2, 2005
Last Updated: March 31, 2011

Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). This module identifies and describes concepts that are needed to understand, plan for, and implement a PKI.

Contents

- [Information About Cisco IOS PKI, page 1](#)
- [Planning for a PKI, page 5](#)
- [Where to Go Next, page 6](#)
- [Additional References, page 6](#)
- [Glossary, page 8](#)

Information About Cisco IOS PKI

Before implementing a basic PKI, you should understand the following concepts:

- [What Is Cisco IOS PKI?, page 2](#)
- [RSA Keys Overview, page 3](#)
- [What Are CAs?, page 3](#)
- [Certificate Enrollment: How It Works, page 4](#)
- [Certificate Revocation: Why It Occurs, page 5](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007, 2008 Cisco Systems, Inc. All rights reserved.

What Is Cisco IOS PKI?

A PKI is composed of the following entities:

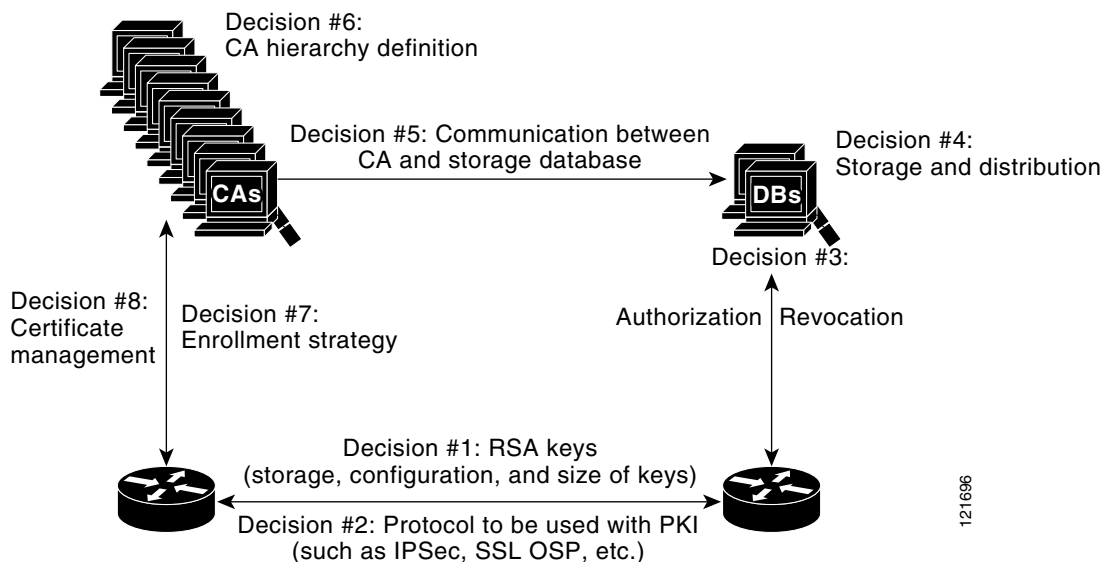
- Peers communicating on a secure network
- At least one certification authority (CA) that grants and maintains certificates
- Digital certificates, which contain information such as the certificate validity period, peer identity information, encryption keys that are used for secure communications, and the signature of the issuing CA
- An optional registration authority (RA) to offload the CA by processing enrollment requests
- A distribution mechanism (such as Lightweight Directory Access Protocol [LDAP] or HTTP) for certificate revocation lists (CRLs)

PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured communication is enrolled in the PKI in a process where the entity generates an Rivest, Shamir, and Adelman (RSA) key pair (one private key and one public key) and has their identity validated by a trusted entity (also known as a CA or trustpoint).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA. When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

Although you can plan for and set up your PKI in a number of different ways, [Figure 1](#) shows the major components that make up a PKI and suggests an order in which each decision within a PKI can be made. [Figure 1](#) is a suggested approach; you can choose to set up your PKI from a different perspective.

Figure 1 *Deciding How to Set Up Your PKI*



RSA Keys Overview

An RSA key pair consists of a public key and a private key. When setting up your PKI, you must include the public key in the certificate enrollment request. After the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, keys with large modulus values take longer to generate, and encryption and decryption operations take longer with larger keys.

What Are CAs?

A CA, also known as a trustpoint, manages certificate requests and issues certificates to participating network devices. These services (managing certificate requests and issuing certificates) provide centralized key management for the participating devices and are explicitly trusted by the receiver to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

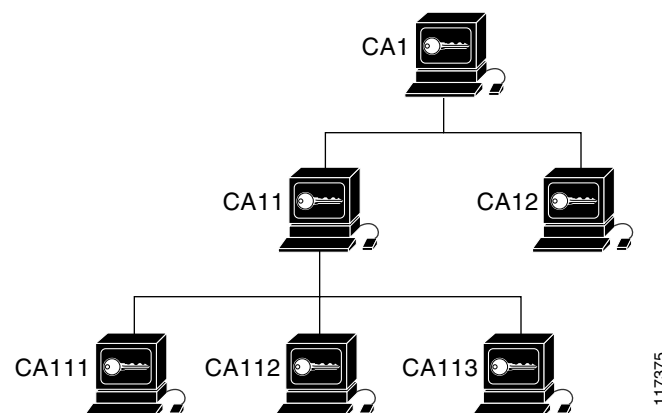
You can use a CA provided by a third-party CA vendor, or you can use an “internal” CA, which is the Cisco IOS Certificate Server.

Hierarchical PKI: Multiple CAs

PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. These enrollment options are how multiple tiers of CAs are configured. Within a hierarchical PKI, all enrolled peers, can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

Figure 2 shows the enrollment relationships among CAs within a three-tiered hierarchy.

Figure 2 Three-Tiered CA Hierarchy Sample Topology



Each CA corresponds to a trustpoint. For example, CA11 and CA12 are subordinate CAs, holding CA certificates that have been issued by CA1; CA111, CA112, and CA113 are also subordinate CAs, but their CA certificates have been issued by CA11.

When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

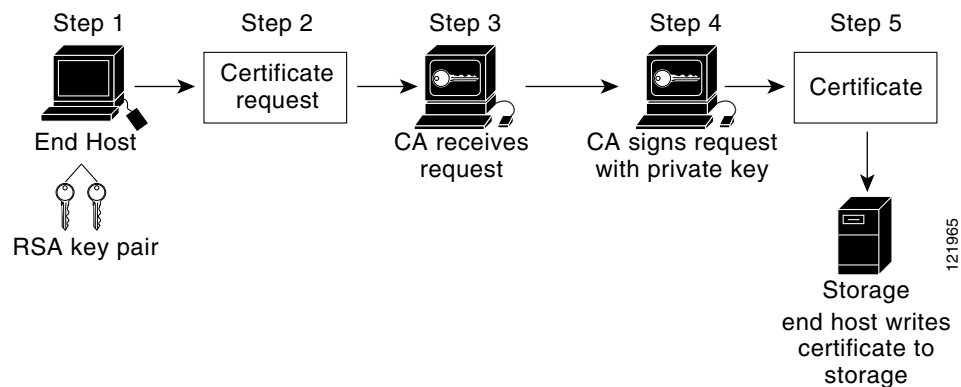
Scenarios in which at least a two-tier CA is recommended are as follows:

- Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the CRLs.
- When online enrollment protocols are used, the root CA can be kept offline with the exception of issuing subordinate CA certificates. This scenario provides added security for the root CA.

Certificate Enrollment: How It Works

Certificate enrollment is the process of obtaining a certificate from a CA. Each end host that wants to participate in the PKI must obtain a certificate. Certificate enrollment occurs between the end host requesting the certificate and the CA. [Figure 3](#) and the following steps describe the certificate enrollment process.

Figure 3 Certificate Enrollment Process



1. The end host generates an RSA key pair.
2. The end host generates a certificate request and forwards it to the CA (or the RA, if applicable).
3. The CA receives the certificate enrollment request, and, depending on your network configuration, one of the following options occurs:
 - c. Manual intervention is required to approve the request.
 - d. The end host is configured to automatically request a certificate from the CA. Thus, operator intervention is no longer required at the time the enrollment request is sent to the CA server.



Note If you configure the end host to automatically request certificates from the CA, you should have an additional authorization mechanism.

4. After the request is approved, the CA signs the request with its private key and returns the completed certificate to the end host.
5. The end host writes the certificate to a storage area such as NVRAM.

Certificate Enrollment Via Secure Device Provisioning

Secure Device Provisioning (SDP) is a web-based certificate enrollment interface that can be used to easily deploy PKI between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server.

SDP (also referred to as Trusted Transitive Introduction [TTI]) is a communication protocol that provides a bidirectional introduction between two end entities, such as a new network device and a Virtual Private Network (VPN). SDP involves the following three entities:

- **Introducer**—A mutually trusted device that introduces the petitioner to the registrar. The introducer can be a device user, such as a system administrator.
- **Petitioner**—A new device that is joined to the secure domain.
- **Registrar**—A certificate server or other server that authorizes the petitioner.

SDP is implemented over a web browser in three phases—welcome, introduction, and completion. Each phase is shown to the user via a web page. For more information on each phase and how SDP works, see the “Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI” module.

Certificate Revocation: Why It Occurs

After each participant has successfully enrolled in the PKI, the peers are ready to begin negotiations for a secure connection with each other. Thus, the peers present their certificates for validation followed by a revocation check. After the peer verifies that the other peer’s certificate was issued by an authenticated CA, the CRL or Online Certificate Status Protocol (OCSP) server is checked to ensure that the certificate has not been revoked by the issuing CA. The certificate usually contains a certificate distribution point (CDP) in the form of a URL. Cisco IOS software uses the CDP to locate and retrieve the CRL. If the CDP server does not respond, the Cisco IOS software reports an error, which may result in the peer’s certificate being rejected.

Planning for a PKI

Planning for a PKI requires evaluating the requirements and expected use for each of the PKI components shown in [Figure 1](#). It is recommended that you (or the network administrator) thoroughly plan the PKI before beginning any PKI configuration.

Although there are a number of approaches to consider when planning the PKI, this document begins with peer-to-peer communication and proceeds as shown in [Figure 1](#). However you or the network administrator choose to plan the PKI, understand that certain decisions influence other decisions within the PKI. For example, the enrollment and deployment strategy could influence the planned CA hierarchy. Thus, it is important to understand how each component functions within the PKI and how certain component options are dependent upon decisions made earlier in the planning process.

Where to Go Next

As suggested in [Figure 1](#), you begin to configure a PKI by setting up and deploying RSA keys. For more information, see the module “Deploying RSA Keys Within a PKI.”

Additional References

Related Documents

Related Topic	Document Title
PKI commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Security Command Reference
Certificate enrollment: supported methods, enrollment profiles, configuration tasks	“ Configuring Certificate Enrollment for a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Certificate revocation and authorization: configuration tasks	“ Configuring Revocation and Authorization of Certificates in a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Cisco IOS certificate server overview information and configuration tasks	“ Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Secure Device Provisioning: functionality overview and configuration tasks	“ Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>
Storing RSA keys and certificates on a USB eToken	“ Storing PKI Credentials ” module in the <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i>

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2459	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
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
RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP
RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema
RFC 2875	Diffie-Hellman Proof-of-Possession Algorithms
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS PKI Overview: Understanding and Planning a PKI

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Glossary

CDP—certificate distribution point. Field within a digital certificate containing information that describes how to retrieve the CRL for the certificate. The most common CDPs are HTTP and LDAP URLs. A CDP may also contain other types of URLs or an LDAP directory specification. Each CDP contains one URL or directory specification.

certificates—Electronic documents that bind a user's or device's name to its public key. Certificates are commonly used to validate a digital signature.

CRL—certificate revocation list. Electronic document that contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when the certificate was issued and when it expires. A new CRL is issued when the current CRL expires.

CA—certification authority. Service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service provides centralized key management for the participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates.

peer certificate—Certificate presented by a peer, which contains the peer's public key and is signed by the trustpoint CA.

PKI—public key infrastructure. System that manages encryption keys and identity information for components of a network that participate in secured communications.

RA—registration authority. Server that acts as a proxy for the CA so that CA functions can continue when the CA is offline. Although the RA is often part of the CA server, the RA could also be an additional application, requiring an additional device to run it.

RSA keys—Public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. An RSA key pair (a public and a private key) is required before you can obtain a certificate for your router.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2005–2011 Cisco Systems, Inc. All rights reserved.