Data Sheet

Cisco IOS Public-Key Infrastructure: Deployment Benefits and Features

Introduction to Public Key Infrastructure

Public Key Infrastructure (PKI) offers a scalable method of securing networks, reducing management overhead, and simplifying the deployment of network infrastructures by deploying Cisco IOS Security protocols, including Cisco IOS IPsec, Secure Shell (SSH), and Secure Socket Layer (SSL). Cisco IOS Software can also use PKI for authorization via access lists and authentication resources. Additional new features build the value-added proposition of Cisco IOS Software to simplify the provisioning and management of Cisco IOS security technologies.

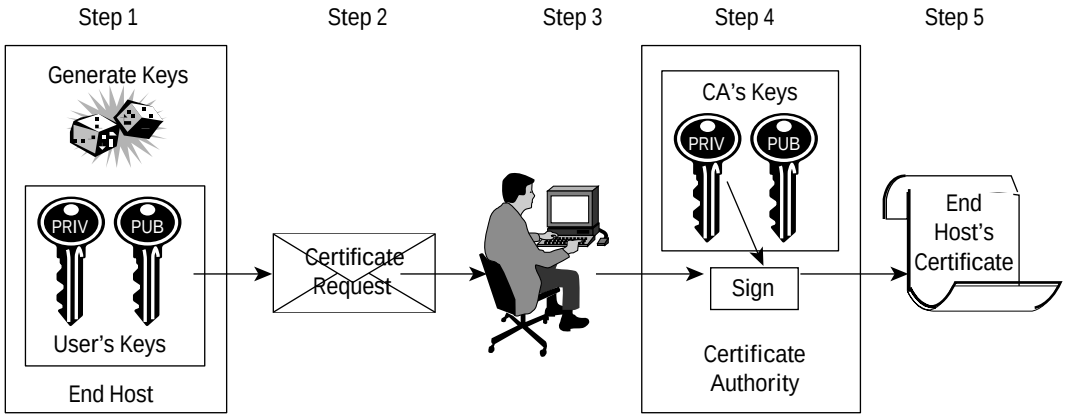
Any network, from small home office routers to the core systems of the world's largest service provider networks, can benefit the enhanced security in Cisco IOS Software.

PKI is a system that manages encryption keys and identity information for the human and mechanical components of a network, which participate in secured communications.

For a person or a piece of equipment to enroll in a PKI, the software on a user's computer generates a pair of encryption keys that will be used in secured communications: a public and a private key. Alternatively, this can be generated by a component of the operating system or functional software on a network device.

The private key is never distributed or revealed; conversely, the public key is freely distributed to any party that negotiates a secure communication. During the enrollment process, the user's public key is sent in the certificate request to the certification authority, which is responsible for the portion of the organization to which that entity belongs. The user sends his public key to the registration component of the Certification Authorities (CA). Subsequently, the administrator approves the request and the CA generates the user's certificate. After the user receives a certificate and installs it on the computer, they can participate in the secured network.

Figure 1
Public Key Infrastructure Enrollment



PKI is used most frequently for encrypted email communications and IPsec tunnel negotiation, which both use the identity and security features of the certificate. The identity components determine the identity of the user, their level of access to the particular type of communication under negotiation, and the encryption information that protects the communication from other parties who are not allowed access. Communicating parties will exchange certificates, and inspect the information presented by the other. The certificates are checked to see if they are within their validity period, and if the certificate was generated by a trusted PKI. If all the identity information is appropriate, the public key is extracted from the certificate and used to establish an encrypted session.

The Case for PKI

There are multiple methods for compromising the security of a network: man-in-the-middle attack, sniffing, tampering, and denial-of-service. Administrators must deploy some combination of encryption and authentication in order to ensure that hackers do not compromise the communications of a secured network. In order to fully leverage most encryption and authentication technologies, key information must be distributed between the components that will manage network security.

Passwords, known as shared secrets, are the simplest way to distribute keys. This requires the configuration of all secured network devices, so that any two devices negotiating a session will have been pre-set with each other's passwords. Shared secrets should be unique, and should be changed periodically in order to ensure continued security. All of these requirements add up to a fairly substantial task to provision and manage shared secrets for encryption. The combination of these requirements is a fairly substantial amount of work, in terms of the provisioning and managing of shared secrets for encryption.

While RSA encryption keys increase encryption security, the network and security operations team still maintain a great deal of responsibility. Administrators must ensure that all devices in the network can communicate, and must manually intervene to ensure that security is maintained if the network is compromised or if it is locked out of a device.

PKI, consisting of one or more CA Server and digital certificates, automates several of these tasks. The CA issues a digital certificate (one time use key) to a device in the network that can authenticate itself to the CA server. Therefore, the process of generating and distributing keys is automated. Certificates are exchanged any time a new session is negotiated, so static pre-shared keys are not configured or stored, enhancing security and reducing administration.

Cisco IOS Software supports interoperability with any X.509 v3 CA to enroll and use digital certificates for traffic authentication and encryption when secure communication is required. By enrolling a Cisco IOS Software device with a CA, the responsibility of managing the security key information is transferred to the network, reducing reliance on people for network security.

Cisco IOS Simplifies Security Infrastructure Deployment and Management

Provisioning and managing a secure network infrastructure becomes much simpler with the Cisco IOS Software PKI Enrollment features.

Provisioning

When deploying a secure network infrastructure, Cisco IOS Software PKI interoperability features reduce the network's engineer's workload by eliminating the need to track cumbersome shared secret lists. The CA interoperability features enables configuration of enrollment so that the router takes care of its enrollment status automatically; in a high-security environment, routers may be enrolled offline with a certificate that is hand-carried or sent via other out-of-band options.

Management—Auto Enrollment

Cisco IOS Software offers features that simplify network management. With the Certificate Auto-Enroll Feature, network devices may be configured to periodically contact the CA and request a new certificate. This reduces the likelihood of network compromise through identity theft. Auto Enrollment may be configured to generate new encryption keys, or continue to use existing keys.

Cisco IOS Public-Key Infrastructure Features to Simplify Deployment and Management

Table 1 PKI Features and Benefits

Feature	Benefit
Certificate Auto-Enroll	Simplifies deployment and management by forcing the router to retrieve digital certificates
Certificate Based Access Control (CBAC)	Centralizes authorization information. A router can extract peer information from a certificate, present it to an AAA server (i.e., RADIUS), and receive an access list to define the access policy for that peer.
N-Tier Certificate Chaining	Allows Cisco IOS Software network devices to operate in a complex PKI environment, where the structure of the PKI is defined by organizational or geographical boundaries.
Manual and TFTP Enrollment	Increases the security of the enrollment process and granularity of control by enabling offline enrollment when the CAs must be closely monitored.

Provisioning and Management Tools

Cisco offers multiple options for PKI provisioning and management, in terms of embedded management and as external management consoles. PKI is currently supported in the VPN Device Manager on routers from the Cisco 1710 to the Cisco 7200 Series Routers. One exception is the Cisco 3700 Series Routers, which will support this in the future.

IP Solution Center offers a scripting interface to provision PKI enrollment on network devices. Another option for managing PKI configuration with regards to IPsec settings may be found in CiscoWorks. The requirements for network device management will dictate the appropriate management platform.

Platform Support

Cisco IOS Software supports PKI functionality on router platforms, beginning with Cisco IOS Software Release 11.3. Support for certificate enrollment and use with Cisco IOS IPsec is available through Cisco IOS Software Release 12.2T. After this release, Cisco enhanced the development cycle of Release 12.2T to increase PKI flexibility and increase the number of enrollment options.

Table 2 Availability

	Platforms	Software
Routers	Cisco 800 Series Cisco ubr900 Series Cisco 1600 Series Cisco 1700 Series Cisco 2600 Series Cisco 3600 Series Cisco 3700 Series Cisco AS5x00 Series Cisco 7100 Series Cisco 7200 Series	Cisco IOS Software Release 12.2(15)T

Cisco 6500 and 7600 Series will support Cisco PKI features as the new security service modules are developed.

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 6317 7777
Fax: +65 6317 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

203031.C/ETMG_04/03