Implementing and Managing PKI Features Roadmap

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

This roadmap lists the public key infrastructure (PKI) features that are documented in the *Cisco IOS Security Configuration Guide: Secure Connectivity* and maps them to the modules in which they appear. For any feature, click the link in the "Where Documented" column to view the module that contains information about the feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for <Phrase Based on Module Title>" section on page 7.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

PKI Feature and Release Support

Table 1 lists PKI feature support for the following Cisco IOS software release trains: Cisco IOS Releases 12.2T, 12.3, and 12.3T.

Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release*.

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

Table 1 Supported PKI Features

Release	Feature Name	Feature Description	Where Documented
12.3(14)T	Administrative Secure Device Provisioning Introducer	This feature lets you act as an administrative introducer to introduce a device into a PKI network and then provide a username as the device name for the record locator in the AAA database.	"*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*" module
12.3(14)T	Persistent Self-Signed Certificates	This feature allows users of the HTTPS server to generate and save self-signed certificates in the router's startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention.	"*Configuring Certificate Enrollment for a PKI*" module
12.3(14)T	Secure Device Provisioning Certificate-Based Authorization	This feature allows certificates issued by other authority (CA) servers to be used for SDP introductions.	"*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*" module
12.3(14)T	Subordinate Certificate Server	This enhancement lets you configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.	"*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*" module
12.3(14)T	USB Storage	This feature lets you store RSA keys on a device external to the router via a USB eToken. The SmartCard technology (which is owned by Aladdin Knowledge Systems) in a USB key form factor (also called a USB eToken) provides secure configuration distribution and lets users store PKI credentials, such as RSA keys, for deployment.	"*Storing PKI Credentials*"
12.3(11)T	Certificate Server Auto Archive	This enhancement enables the CA certificate and CA key to be backed up automatically just once after they are generated by the certificate server. As a result, you do not need to generate an exportable CA key if CA backup is desirable.	"*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*" module
12.3(11)T	PKI AAA Authorization Using the Entire Subject Name	This feature lets users query the AAA server using the entire subject name from the certificate as a unique AAA username.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module
12.3(11)T	PKI Status	This feature adds the **status** keyword to the **show crypto pki trustpoints** command, which lets you view the current status of the trustpoint. Before this feature, you had to issue the **show crypto pki certificates** and the **show crypto pki timers** commands for the current status.	"*Configuring Certificate Enrollment for a PKI*" module
12.3(11)T	Re-Enroll Using Existing Certificates	This feature lets users re-enroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.	"*Configuring Certificate Enrollment for a PKI*" module
12.3(8)T	Easy Secure Device Deployment	This feature introduces support for SDP (formerly called EzSDD), which offers a web-based enrollment interface that lets network administrators deploy new devices in large networks.	"*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*" module

Table 1 Supported PKI Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.3(8)T	Easy Secure Device Deployment AAA Integration	This feature integrates an external AAA database, which allows the introducer to be authenticated against a AAA database instead of using the enable password of the local Cisco certificate server.	"*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*" module
12.3(7)T	Certificate Server Registration Authority (RA) Mode	A certificate server can be configured to run in RA mode.	"*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*" module
12.3(7)T	The **crypto pki** commands should be a synonym for **crypto ca** commands	This enhancement changes all commands that begin as **crypto ca** to **crypto pki**. Although the router still accepts **crypto ca** commands, all output is read back as **crypto pki** commands.	All modules that contain **crypto ca** commands.
12.3(7)T	Key Rollover for Certificate Renewal	This feature allows the certificate renewal request to be made before a certificate expires. The old key and certificate is retained until the new certificate is available.	"*Configuring Certificate Enrollment for a PKI*" module
12.3(7)T	PKI: Query Multiple Servers During Certificate Revocation Check	This feature lets Cisco IOS software make multiple attempts to retrieve the CRL, which allows operations to continue when a particular server is not available. Also, this feature lets you override the CDPs in a certificate with a manually configured CDP. Manually overriding the CDPs in a certificate can be advantageous when a particular server is unavailable for a long period of time. The certificate's CDPs can be replaced with a URL or directory specification without reissuing all of the certificates that contain the original CDP.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module
12.3(7)T	Protected Private Key Storage	This feature lets a user encrypt and lock the RSA private keys that are used on a Cisco IOS router, which prevents unauthorized use of the private keys.	"*Deploying RSA Keys Within a PKI*" module
12.3(4)T	Import of RSA Key Pairs and Certificates in PEM Format	This feature lets users use PEM-formatted files to import or export RSA key pairs. PEM-formatted files let customers directly use existing RSA key pairs on their Cisco IOS routers instead of generating new keys. Also, users can issue certificate requests and receive issued certificates in PEM-formatted files.	"*Deploying RSA Keys Within a PKI*" module and "*Configuring Certificate Enrollment for a PKI*" module
12.3(4)T	Using Certificate ACLs to Ignore Revocation Check and Expired Certificates	This feature allows a certificate that meets specified criteria to be accepted regardless of the validity period of the certificate, or if the certificate meets the specified criteria, revocation checking does not have to be performed. Certificate ACLs are used to specify the criteria that the certificate must meet to be accepted or to avoid revocation checking. In addition, if AAA communication is protected by a certificate, this feature allows the AAA checking of the certificate to be ignored.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module

Table 1 Supported PKI Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.3(4)T	Cisco IOS Certificate Server	This feature introduces support for the Cisco IOS CS, which offers users a CA that is directly integrated with Cisco IOS software to deploy basic PKI networks more easily.	"*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*" module
12.3(4)T	Direct HTTP Enrollment with CA Servers	This feature lets users configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA as a proxy. The enrollment profile lets users send HTTP requests directly to the CA server instead of the RA proxy.	"*Configuring Certificate Enrollment for a PKI*" module
12.3(2)T	Online Certificate Status Protocol (OCSP)	This feature lets users enable OCSP instead of CRLs to check certificate status. Unlike CRLs, which provide only periodic certificate status, OCSP can provide timely information regarding the status of a certificate.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module
12.3(1)	PKI Integration with AAA Server	This feature provides additional scalability for authorization by generating a AAA username from the certificate presented by the peer. A AAA server is queried to determine whether the certificate is authorized for use by the internal component. The authorization is indicated by a component-specified label that must be present in the AV pair for the user.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module
12.2(15)T	Certificate Security Attribute-Based Access Control	Under the IPsec protocol, CA interoperability permits a Cisco IOS device and a CA to communicate so that the device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. This feature adds fields to the certificate that allow specifying an ACL in order to create a certificate-based ACL.	"*Configuring Authorization and Revocation of Certificates in a PKI*" module
12.2(15)T	Exporting and Importing RSA Keys	This feature lets you transfer security credentials between devices by exporting and importing RSA keys. The key pair that is shared between two devices allows one device to immediately and transparently take over the functionality of the other router.	"*Deploying RSA Keys Within a PKI*" module
12.2(15)T	Multiple-Tier CA Hierarchy	This enhancement lets users set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA.	"*Configuring Certificate Enrollment for a PKI*" module
12.2(13)T	Manual Certificate Enrollment (TFTP Cut-and-Paste)	This feature lets users generate a certificate request and accept CA certificates as well as the router's certificates via a TFTP server or manual cut-and-paste operations.	"*Configuring Certificate Enrollment for a PKI*" module
12.2(8)T	Certificate Autoenrollment	This feature introduces certificate autoenrollment, which lets the router automatically request a certificate from the CA that is using the parameters in the configuration.	"*Configuring Certificate Enrollment for a PKI*" module

Table 1 Supported PKI Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.2(8)T	Certificate Enrollment Enhancements	This feature introduces five new **crypto pki trustpoint** subcommands that provide new options for certificate requests and let users specify fields in the configuration instead of going through prompts.	"*Configuring Certificate Enrollment for a PKI*" module
12.2(8)T	Multiple RSA Key Pair Support	This feature lets users configure a router to have multiple RSA key pairs. Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.	"*Deploying RSA Keys Within a PKI*" module
12.2(8)T	Trustpoint CLI	This feature introduces the **crypto pki trustpoint** command, which adds support for trustpoint CAs.	"*Configuring Certificate Enrollment for a PKI*" module