Certificate Authority Support for IPSec Overview

Cisco offers many technologies to choose from in building a custom security solution for Internet, extranet, intranet, and remote access networks. These scalable solutions seamlessly interoperate to deploy enterprise-wide network security. Cisco offers comprehensive support for perimeter security, user authentication, accounting, and data privacy. Cisco's IP Security(IPSec) delivers a key technology component for providing this total security solution.

IPSec scalability, the ability to deploy large (greater than 100 node) IPSec networks, has been one of the greatest challenges facing early implementers of network-layer encryption. Digital certificate technology provides the ability for devices to easily authenticate each other in a manner that scales to very large networks.

Many organizations are currently implementing a public key infrastructure (PKI) for managing digital certificates across a wide variety of applications, including virtual private networks(VPNs), secure electronic mail, secure web access, and other applications that require security. Cisco's implementation of IPSec is interoperable with several leading PKI vendors. This scenario enables you to choose the best PKI for your individual needs, while knowing that it will be compatible with Cisco's network security solutions.

Introduction to Digital Certificates

One of the key challenges faced when deploying an encryption system is how to authenticate the other party with whom you are communicating. The whole point of encryption is to ensure the confidentiality of your information. If an attacker is able to convince you that he should be trusted, and you send him a stream of encrypted data that he can decrypt, then you have just wasted your effort-and lost the privacy of your information. It is of utmost importance that you know to whom you are sending encrypted data before you send it.

Digital signatures, enabled by public key cryptography, provide a means to digitally authenticate devices and individual users. In public key cryptography, such as the RSA encryption system, each user has a key pair that contains both a public and a private key. The keys act as complements-anything encrypted with one of the keys can be decrypted with the other. In simple terms, a signature is formed when data is encrypted with a sender's private key. The receiver verifies the signature by decrypting the message with the sender's public key. The fact that the message could be decrypted using the sender's public key indicates that the holder of the private key, the sender, must have created the message. This process relies on the receiver having a copy of the sender's public key and knowing with a high degree of assurance that it really does belong to the sender, and not to someone pretending to be the sender.

Digital certificates provide this assurance. A digital certificate contains information to identify a user or device, such as the name, serial number, company, department or IP address. It also contains a copy of the public key of the entity. The certificate is signed by a certification authority (CA)-a third party that is explicitly trusted by the receiver to validate identities and to create digital certificates.

CISCO SYSTEMS

There is a sort-of "chicken-and-egg" problem with this scheme. In order to validate the CA's signature, the receiver must first know the CA's public key. Normally this process is handled out of band or through an operation done at installation. For instance, most web browsers are preconfigured with the public keys of several CAs by default.

The Internet Key Exchange (IKE), a key component of the IPSec solution, can use digital signatures to scalably authenticate peer devices before setting up security associations. Without digital signatures, users must either manually exchange public keys or secrets between each pair of devices that use IPSec to protect communications. Without certificates, whenever a new device is added to the network, users are required to make a configuration change on every other device it securely communicates with. However, by using digital certificates, users simply enroll each new device with a certificate authority. When two devices wish to communicate, they exchange certificates and each digitally signs some data to authenticate each other. When a new device is added to the network, users simply enroll that device with a CA-none of the other devices need modification. When the new device attempts an IPSec connection, IKE automatically exchanges certificates with the peer and the devices authenticate to each other.

Cisco's Support of Digital Certificates

Cisco fully supports the use of digital certificates by IKE and implements the following standards:

- X.509v3—the standard certificate format; it specifies how to form a certificate.
- CRLv2—the certificate revocation list, version 2; it is a list of revoked certificates, that is, certificates that should no longer be trusted.
- Certificate Enrollment Protocol (CEP)—a certificate management protocol jointly developed by Cisco Systems and VeriSign, Inc. CEP is an early implementation of Certificate Request Syntax (CRS), a standard proposed to the Internet Engineering Task Force (IETF). CEP specifies how a device communicates with a CA, including how to retrieve the CA's public key, how to enroll a device with the CA, and how to retrieve a Certificate revocation list (CRL). CEP uses RSA's PKCS (public key cryptography standards) 7 and 10 as key component technologies. The IETF's public key infrastructure working group (PKIX) is working to standardize a protocol for these functions, either CRS or an equivalent. When an IETF standard is stable, Cisco will add support for it.

Vendor Support

Cisco is working with several leading PKI vendors, including VeriSign, Inc. and Entrust Technologies to provide support for the CEP. Details of the support provided by each vendor follows. Cisco is currently working with other vendors and will add them to this list when their CEP support is complete.

Verisign, Inc.: VeriSign OnSite for IPSec

VeriSign, Inc., is the leading provider of digital certificate solutions for extranets and intranets, including IPSec. VeriSign OnSite for IPSec enables organizations to easily issue certificates and build their own virtual private networks (VPNs) using the IPSec capabilities built into Cisco products.

VeriSign OnSite for IPSec combines VeriSign's turnkey certificate authority software with the company's robust, mission-critical certificate processing and management services, providing enterprises with a complete PKI. Because of its unique configuration, the unique combination of service and software of VeriSign OnSite makes it easy for companies to be their own CA without an expensive and time-consuming process.

Corporate OnSite administrators who configure the system completely control the functioning of the service and the issuing of certificates, while VeriSign maintains the back-end service, performs backups, operates the hardware, and performs other day-to-day operational tasks. The corporate administrators running the system simply need to use Microsoft Internet Explorer or Netscape Navigator / Communicator Web browsers, versions 4.0 or higher. The product also comes with an OnSite Administrator Certificate, stored on a smart card, to securely manage IPSec certificate administration.

Additional information on VeriSign's IPSec products, services, pricing, and evaluation versions can be found at `http://www.verisign.com/ipsec/index.html`.

Entrust Technologies: Entrust/VPN Connector

Entrust Technologies, Inc., (Nasdaq: ENTU), the worldwide leader in managed PKI solutions provides the easiest and most effective means of implementing certificate-based VPN solutions. Entrust's solutions were chosen for the Automotive Industry Action Group's (AIAG) Automotive Network eXchange (ANX) interoperability trials for their ability to support the broadest range of VPN devices in the industry today.

An important component of the Entrust VPN product line is the Entrust/VPN Connector. Designed to support Cisco's CEP, the Entrust/VPN Connector enrolls CEP-enabled devices from the same Entrust PKI that automatically manages certificate services for over 100 other security applications in over 600 customers globally. Managed PKI applications include desktop file encryption and signing applications, secure e-mail, web, form-flow, time stamp, and now IPSec-based VPN implementations.

Additional information on Entrust's products, services, and test drives can be found at http://www.entrust.com or call 888-690-2424.

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

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
http://www-europe.cisco.com
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

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

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
http://www.cisco.com
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Connection Online Web site at http://www.cisco.com/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong • 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 • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela