Symantec™ Device Certificate Service

Data Sheet: Authentication

Service providers are continually striving to prevent unauthorized access to their valuable networks and services. This level of security requires authenticating the identity of hardware devices that attempt access to networked services. Security solutions based on Public Key Infrastructure (PKI) are particularly well-suited to address identity authentication for distributed hardware devices. PKI platforms are based on a trusted Certification Authority (CA) that issues, renews, revokes, and manages digital certificates used for valid identification. To secure identity, PKI-based digital certificates are embedded onto devices during assembly, and communicate with a service provider to authenticate access to a service.

A prime example of PKI use to authenticate identity in hardware devices is the practice adopted by the cable industry. To protect their networks and their customers, the cable industry requires that devices such as cable modems, set-top boxes, and televisions employ embedded PKI digital certificates in order to be compliant. The digital certificates perform device authentication with a cable operator's back-end services before being granted access. This PKI-based security practice has succeeded in mitigating cloning of customer premise equipment and pirating of cable operator services.

Symantec™ Device Certificate Service

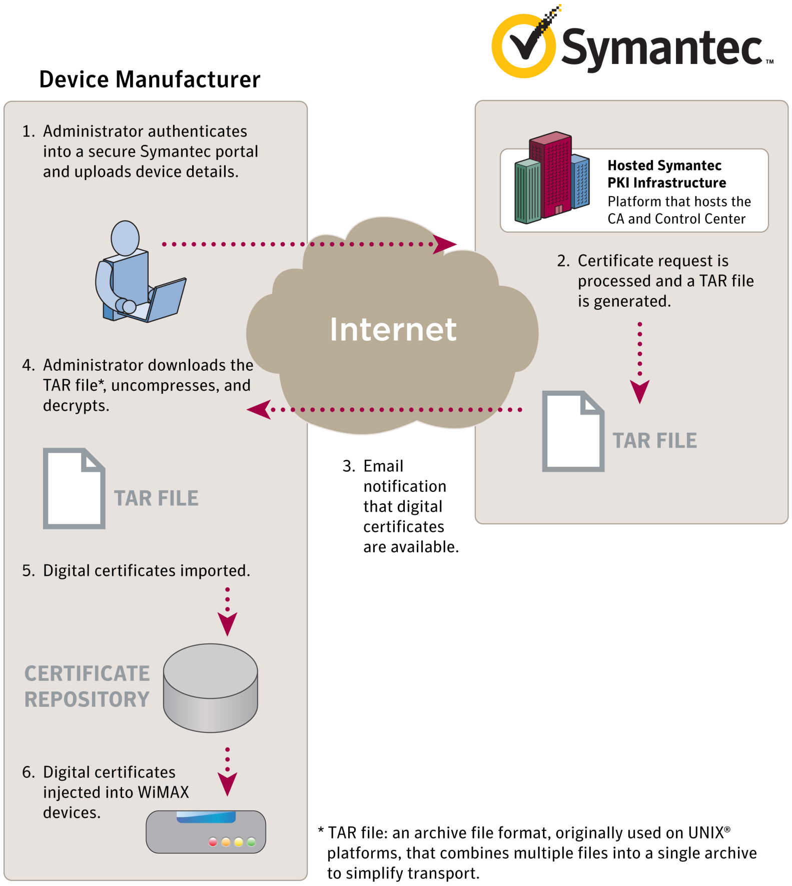
Symantec™ Device Certificate Service delivers a fast, efficient, and cost-effective means to embed PKI-based digital certificates into any type of hardware device, including cable modems, set-top boxes, integrated digital televisions, digital-cable-ready televisions, ATMs, networking devices, or WiMAX-compliant subscriber stations. Symantec provides device manufacturers with a turn-key solution for generating batches of digital certificates through an easy-to-use Web interface. Technical knowledge of PKI is not required, nor is investment in expensive infrastructure to manage the authentication service. The PKI environment is fully hosted and managed by Symantec in a 24 hours a day, seven days a week, 365 days a year secure facility, enabling the service provider or device manufacturer to focus on their core business.

Proven, trust-based security

With Symantec PKI-based digital certificates embedded in the hardware devices, service providers mitigate fraud by performing authentication on the distributed devices used by their subscribers. This PKI-based authentication helps prevent rogue devices, employed by unauthorized users from accessing services such as cable network-based Voice Over IP (VOIP), digital media content, high definition, or other broadband services. Over 200 million devices worldwide currently depend on Symantec PKI-based digital certificates to provide security for accessing networked services, making Symantec the leader in securing industry ecosystems and powering trust communities.

Device Certificate Service delivers:

- **Ease of deployment**– Digital certificates are ordered in bulk by providing Symantec with a list of media access controller (MAC) addresses, or unique device IDs. Device Certificate Service generates the PKI digital certificates and securely delivers them to the manufacturers for inclusion on their devices.
- **Certificate lifecycle management**– Certificate lifecycle management consists of request, issuance, usage, renewal, and validation of the device certificates. Device Certificate Service performs these functions on behalf of the device manufacturer.


Symantec
Device Manufacturer
1. Administrator authenticates into a secure Symantec portal and uploads device details.
Hosted Symantec PKI Infrastructure
Platform that hosts the CA and Control Center
2. Certificate request is processed and a TAR file is generated.
Internet
TAR FILE
3. Email notification that digital certificates are available.
4. Administrator downloads the TAR file*, uncompresses, and decrypts.
TAR FILE
5. Digital certificates imported.
CERTIFICATE REPOSITORY
6. Digital certificates injected into WiMAX devices.

* TAR file: an archive file format, originally used on UNIX® platforms, that combines multiple files into a single archive to simplify transport.

Figure 1: Device certificate deployment process

Flexible management

Device Certificate Service provides flexibility in how a service provider manages its trust environment. CAs can have blanket coverage, or be granted specific zones of influence that derive behavior from the root CA—the highest level of PKI trust issued for device certificates. These sub-CAs are derived from the root CA and are used to establish a separate domain of trust that can be segregated within the root CAs' community. For example, a particular device manufacturer may want to create its own sub-CA to issue certificates specific to a given service provider. In such a scenario, only devices with digital certificates issued under that sub-CA will be trusted by the designated service provider.

Device Certificate Service offers design, establishment, and hosted management of a trust hierarchy based on a CA. Symantec also provides:

- **Certificate policy** that define roles, responsibilities, and usage for PKI-based digital certificates.
- **Certificate practice statements** that define how a certificate policy will be implemented for the establishment and operation of the PKI-based solution—these can also be modified by the device manufacturer to meet custom needs.

Features and benefits

Feature	Benefit
Cost-effective and easy-to-use hosted service	By leveraging Device Certificate Service, and its extensive PKI infrastructure, device manufacturers save significantly versus implementing and managing their own PKI environment. • Turn-key service for device manufacturers. • Delivers quick activation turnaround and an easy-to-use Web interface for certificate request and download.
World-class professional and support services	Symantec Professional and Support Services alleviate the burden of planning, implementing, and maintaining an in-house, full-scale support infrastructure. • Symantec Support Services can devote more resources to state-of-the-art PKI technology, security, and training than is feasible for most device manufacturers.
Reliable security	Employs the same PKI technology that is used throughout Symantec's military-grade PKI and Network Operations Centers. • Supports 24x7x365 monitoring, management, and escalation across the globe with full disaster recovery. • Annual WebTrust™ and SAS-70 compliance audits are conducted by an independent, accredited third-party.
Carrier-class scalability	Architected to support the highest volume and peak load requirements in the industry. • Overall system architecture is designed to support the issuance and management of over 100 million certificates per year. • Symantec diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.
Rapid deployment	Device manufacturers can be receiving batches of PKI-based digital certificates within days of signing up for Device Certificate Service.

More Information

Visit our website

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

350 Ellis St., Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934
www.symantec.com

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.