



DATA SHEET



KEY FEATURES

24/7 Support

Our DCS support services consist of interactive online help and staffed services. VeriSign's customer support staff has the expertise in supporting more than 300,000 Web Sites and 1,000 organizations.

Secured Facilities and Personnel

Leverage VeriSign's operations support investment and unmatched real-life PKI support expertise, saving the cost of recruiting, training, and maintaining in-house support personnel.

Highly Scalable

With the current capacity to issue 70 million certificates per year, VeriSign® Device Certificate Service can grow with your business and easily accommodate requests for increasing numbers of digital certificates as production expands.

Fast and Easy-to-Use Hosted Service

VeriSign® Device Certificate Service presents quick activation turnaround and an easy-to-use web interface for certificate request and download.

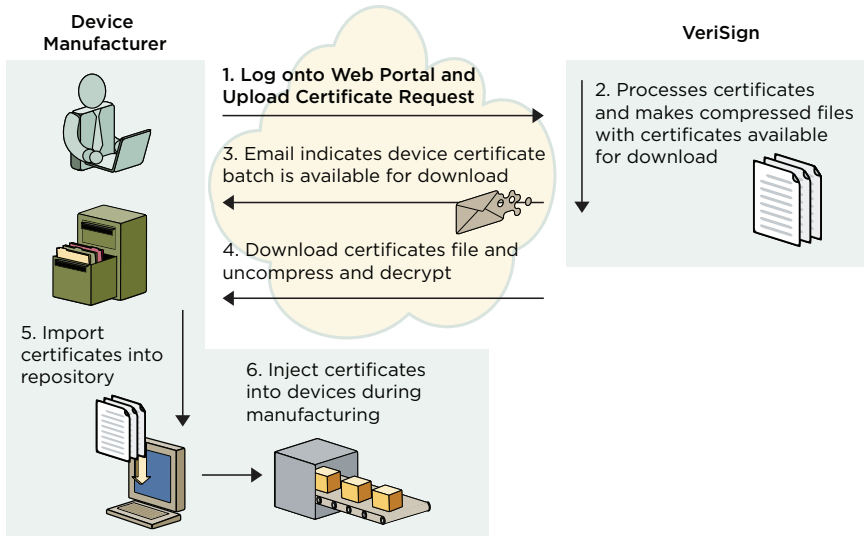
VeriSign® Device Certificate Service

The need to authenticate all hardware devices accessing networked services is on the rise as businesses continually strive to prevent unintended devices from gaining access to protected networks and services. One pioneering example is the authentication practice adopted by the cable industry where Data Over Cable Service Interface Specifications (DOCSIS) compliant cable modems, set-top boxes and OpenCable-compliant televisions employ embedded X.509-standard certificates to perform device authentication to cable operators' networked backend services before being granted access. The specific security practice within the cable industry has minimized both cloning of customer-premise equipments (CPEs) and pirating of cable operator services. In particular, the DOCSIS BPP+ (Baseline Privacy Plus) interface specification, which details the elements of X.509 certificate-based device authentication, has been widely modeled in other industry applications such as the authentication of WiMAX-standard CPEs.

The VeriSign® Device Certificate Service makes it fast, efficient, and cost-effective to embed X.509 certificates into any type of hardware devices such as cable modems, set-top boxes, Digital-Cable-Ready televisions, or WiMAX-compliant subscriber stations. The X.509-standard certificates embedded in the hardware devices enable service providers to perform strong authentication of their distributed devices used by their subscribers. The certificate-based authentication prevents any rogue device employed by unauthorized users from accessing services such as cable network based VOIP, digital media content, or broadband service. VeriSign provides hardware device manufacturers with a turnkey solution for generating batches of digital certificates and private keys through an easy-to-use Web interface without requiring hardware manufacturers to master X.509-based certificate security technology or invest in expensive infrastructure as the service is completely hosted at VeriSign's 24x7 secure data center facility.



Where it all comes together.™



+ Device Certificate Request & Issuance Overview

With the VeriSign® Device Certificate Service, device manufacturers order certificates in bulk by providing VeriSign with a list of MAC addresses or unique device IDs for the certificates. The manufacturers may either supply VeriSign with pre-generated public-keys, or may allow VeriSign to generate the private-public key pairs for the certificates. VeriSign securely returns the issued certificates encrypted to the manufacturers.

+ Certificate Lifecycle Management

Certificate lifecycle management primarily consists of request, issuance, usage, renewal and validation of the device certificates. With VeriSign® Device Certificate Service, this lifecycle can be achieved in a few easy steps. The following describes a typical device certificate request and issuance scenario.

1. The device manufacturer’s administrator logs in to the secure VeriSign hosted Device Certificate Service Web portal and upload a certificate request file (text format) containing the list of MAC addresses or serial numbers for the devices.
2. The VeriSign® Device Certificate Service processes the certificate request file and creates a compressed tar file containing all issued certificates in the “Download” section of the Web portal.
3. An email from VeriSign informs the device manufacturer’s administrator that the batch of issued device certificates are available for download.
4. The device manufacturer’s administrator downloads the compressed tar file containing the issued certificates and uses the VeriSign-provided “uncompress and decrypt” utility to open the compressed tar file.
5. The device manufacturer administrator imports the resulting X.509 certificates into the manufacturer’s certificate repository (e.g., database).
6. The device manufacturer incorporates the process of injecting the certificates into the target devices as part of its overall device manufacturing process.

+ Certification Authority (CA) Management

The VeriSign® Device Certificate Service includes design and establishment of the CA structure for the right trust hierarchy, and optionally the corresponding Certificate Policy (CP) and Certificate Practices Statements (CPS) for the establishment and operation of the PKI system. The root CA represents the highest level of PKI trust for its sub-CAs and the device certificates issued. Consequently, it is extremely critical that it resides in a highly secure hardware storage and facility environment. As an industry pioneer and leader in PKI, VeriSign uses a proven, secure, auditable process to design, create, and store the root CA and its sub-CAs at its secure data center.

The sub-CA establishes a separate domain of trust within the root CA's community. For example, a particular device manufacturer may want to create its own sub-CA and issue manufacturer-specific certificates under that sub-CA. This would allow only devices with certificates issued under that sub-CA to be trusted by a particular service provider. If you expect your certificates to be used and relied upon by an open community of users, it is recommended that you have a public-accessible written CP and CPS to inform the community of users about your certificate policy and practices.

+ Optional Certificate Revocation Service

Certificate status checking is required when a relying party needs to verify the status of a certificate used for the authentication process. The goal of certificate status checking is simply to verify that the certificate has not been revoked at the time of validation. If your PKI application requires real-time certificate status checking besides the trust validation of the certificate chain, you may choose to subscribe to VeriSign's certificate status validation service via Certificate Revocation List (CRL). Specifically, the relying party (via the PKI application) checks the corresponding CRL specified in the certificate to see if the certificate in question is listed in the CRL. If it is, the certificate is deemed "revoked" and hence wouldn't be trusted.

With VeriSign Device Certificate Service, revoking a certificate is a simple process. The Device Certificate Service administrator logs into the Web portal and uploads a revocation request file containing a list of certificate serial numbers to be revoked.

+ To Learn More

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit www.verisign.com/products/pki.

Visit us at www.Verisign.com for more information.