



DATA SHEET



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.

VeriSign® Device Certificate Service

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, or 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.

+ VeriSign Device Certificate Service

VeriSign 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, digital-cable-ready televisions, ATMs, networking devices, or WiMAX-compliant subscriber stations. VeriSign 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 VeriSign in a 24x7x365 secure facility, enabling the service provider to focus on their core business.

Proven, Trust-based Security

With VeriSign 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 VOIP, digital media content, or broadband services. Over 80 million devices worldwide currently depend on VeriSign's PKI-based digital certificates to provide security for accessing networked services, making VeriSign the leader in securing industry ecosystems and powering trust communities.

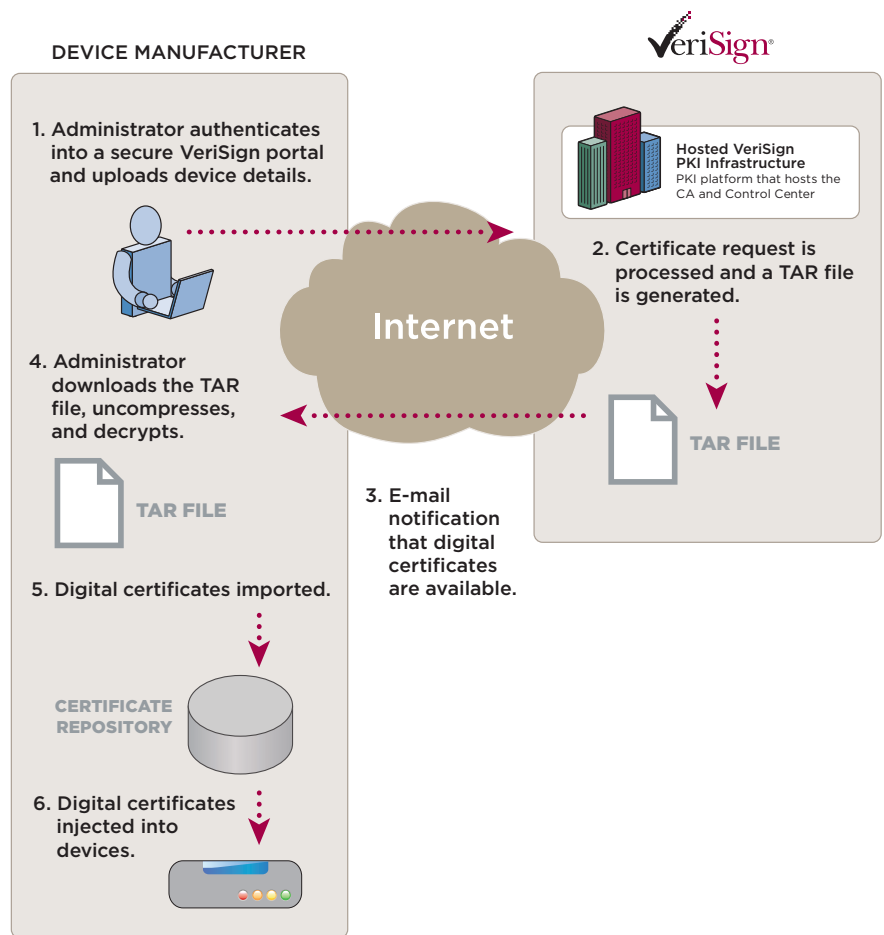
VeriSign Device Certificate Service delivers:

- **Ease of Deployment** – Digital certificates are ordered in bulk by providing VeriSign with a list of MAC addresses, or unique device IDs. VeriSign 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. VeriSign Device Certificate Service performs these functions on behalf of the device manufacturer.



Figure 1: Device Certificate Deployment Process

1. The device manufacturer's administrator logs in to the secure Web portal and uploads a certificate request file (text format) that contains the list of MAC addresses or unique IDs for the devices. Alternatively, the device manufacturer can submit a batch of PKCS#10-formatted Certificate Signing Requests (CSRs).
2. VeriSign processes the certificate request file and generates a compressed TAR file containing all issued digital certificates, and optionally the private keys (when the request is based on MAC addresses or other unique IDs)
3. An email from VeriSign informs the device manufacturer's administrator that the batch of issued digital certificates is available for download.
4. The administrator downloads the compressed TAR file and uses the VeriSign-provided "uncompress and decrypt" utility to receive all the digital certificates (and, optionally, private keys).
5. The administrator imports the resulting digital certificates into the manufacturer's certificate repository (i.e., a database).
6. The device manufacturer injects the PKI-based digital certificates into the target devices during the manufacturing process.



+ Flexible Management

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

VeriSign Device Certificate Service offers design, establishment, and hosted management of a trust hierarchy based on a Certification Authority. VeriSign 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 & Benefits

Cost-Effective and Easy-to-Use Hosted Service	<p>By leveraging VeriSign Device Certificate Service, and its extensive PKI infrastructure, device manufacturers save significantly versus implementing and managing their own PKI environment.</p> <ul style="list-style-type: none">• 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	<p>VeriSign's Professional and Support Services alleviate the burden of planning, implementing, and maintaining an in-house, full-scale support infrastructure.</p> <ul style="list-style-type: none">• VeriSign 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	<p>Employs the same PKI technology that is used throughout VeriSign's military-grade public key infrastructure and Network Operations Centers.</p> <ul style="list-style-type: none">• 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	<p>Architected to support the highest volume and peak load requirements in the industry.</p> <ul style="list-style-type: none">• Overall system architecture is designed to support the issuance and management of over 100 million certificates per year.• VeriSign's diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.
Rapid Deployment	<p>Device manufacturers can be receiving batches of PKI-based digital certificates within days of signing up for VeriSign Device Certificate Service.</p>

+ Learn More

For more information about VeriSign Device Certificate Service, please call 650-426-5310 or visit: www.verisign.com/authentication

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