



DATA SHEET



VeriSign® WiMAX Public Key Infrastructure Service for Device Manufacturers

WiMAX is a collection of integrated wireless broadband technologies and products built around the harmonized IEEE 802.16e/ETSI HiperMAN standard. Ensuring secure communication over WiMAX-based networks is a critical success factor for the growth of the WiMAX ecosystem. Seamless security that is transparent to the end user is also crucial for widespread adoption. Security solutions based on Public Key Infrastructure, or PKI, are particularly well-suited in addressing these business needs.

PKI platforms are based on a trusted Certification Authority (CA) that issues, renews, revokes, and manages digital certificates used for valid identification. PKI delivers strong authentication—also known as “two-factor authentication”—to ensure that valid devices are properly authenticated for access to a service. Strong authentication provides an additional layer of protection beyond traditional access methods, such as the relatively vulnerable username/password. Solutions using PKI digital certificates are also relatively transparent as they can be embedded on devices and do not require interaction from the end user to authenticate identity.

+ VeriSign WiMAX PKI Service

VeriSign WiMAX Public Key Infrastructure (PKI) Service for device manufacturers is a hosted solution that is managed by VeriSign and enables secure communication over WiMAX-based wireless networks.

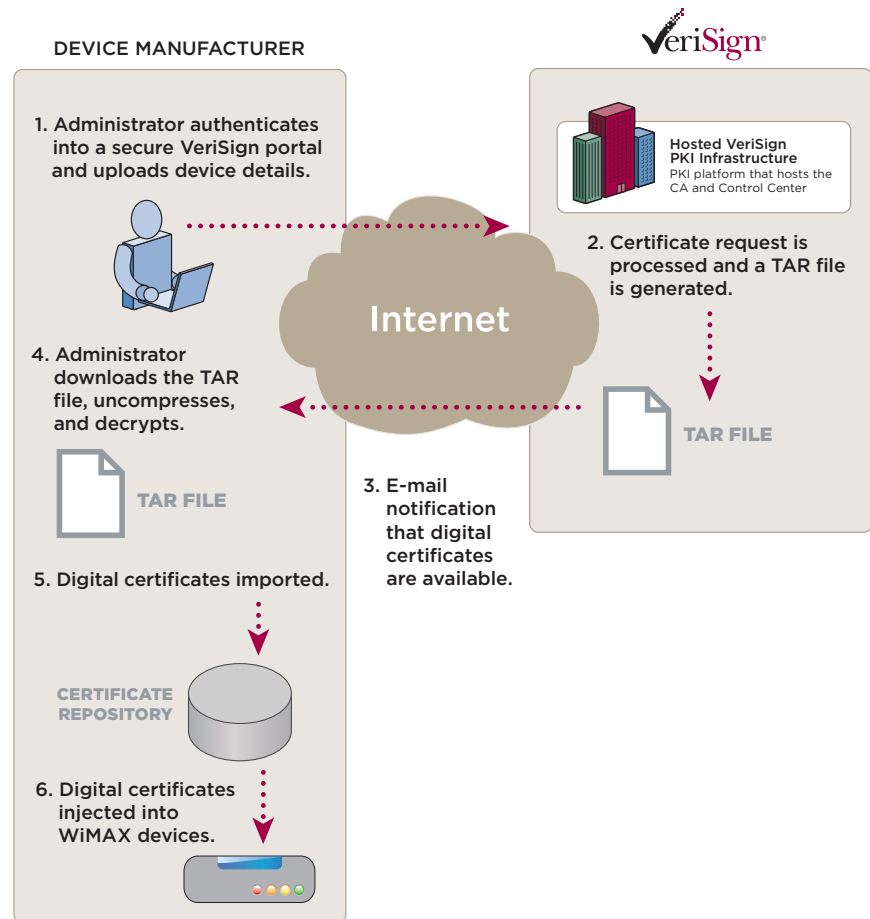
A Proven PKI Platform for Device Manufacturers

VeriSign WiMAX PKI Service delivers a fast and efficient means to embed PKI-based digital certificates into any type of WiMAX-compliant subscriber station or device. It inherits industry-leading functionality from VeriSign Device Certificate Service, and offers a best-in-class solution for the WiMAX Device PKI. Over 80 million devices worldwide depend on VeriSign’s PKI-based digital device certificates to secure access to services, making VeriSign the leader in powering trust in communities such as the WiMAX ecosystem.



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 WiMAX devices during the manufacturing process.



VeriSign WiMAX PKI 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 then generates the PKI-based digital certificates and securely delivers them to the manufacturers for inclusion on their devices.
- **Certificate Lifecycle Management** – Certificate Lifecycle Management consists of request, issuance, and validation of the device certificates. VeriSign WiMAX PKI Service performs these functions on behalf of the device manufacturer.
- **Flexible Management of Trust Environments** – VeriSign WiMAX PKI Service can optionally provide the device manufacturer a signed sub-Certification Authority (CA) for autonomous operations. Use of these sub-CAs enables the device manufacturer to run certificate lifecycle management and CRL hosting and create its own zone of influence in the trust ecosystem.

VeriSign for WiMAX PKI Service is capable of supporting millions of end user PKI-based WiMAX digital certificates on a global scale.

+ Features & Benefits

Hosted Certification Authority (CA)	VeriSign hosts and operates a Certification Authority that enables enterprises to achieve lower total cost of ownership than stand-alone in-house PKI implementations, and has the following functionality: <ul style="list-style-type: none">• Generation of Certificate Authority key pairs.• Activation and deactivation of Certificate Authority certificates.• Maintenance of Certificate Revocation Lists (CRLs).
Registration Authority (RA)	Allow administrators to: <ul style="list-style-type: none">• Authenticate, approve, or reject certificate requests from subscribers, and revoke certificates.• Generate reports on certificate activity.
Mission-Critical Reliability	Employs the same PKI technology that is used throughout its military-grade public key infrastructure and Network Operations Centers. <ul style="list-style-type: none">• Supports 24x7x365 monitoring, management, and escalation across the globe with full disaster recovery.• Certified annually by KPMG as part of a SAS-70 security audit. A regular WebTrust audit of VeriSign's PKI infrastructure is also conducted.
Scalable	Architected to support the highest volume and peak load requirements in the industry. <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.
Future-Ready	VeriSign has a strong commitment to open standards, innovative technology, and strategic collaborations to enable the flexibility needed to evolve with the changing technology landscape. <ul style="list-style-type: none">• Supports standard certificate types, including: S/MIME, SSL, and IPSec, as well as PKI industry standards such as X.509 v3, LDAP, and PKCS #7, PKCS #10, and PKCS #12.• VeriSign's open approach to security enables organizations to operate freely in diverse environments, and maximize return on, and preservation of, existing investments.
World-Class Service	VeriSign provides binding service-level agreements that include high-security facilities with: <ul style="list-style-type: none">• Highly trained, trusted personnel• Redundant systems• 24x7x365 customer support• Disaster recovery• Full audit and archiving
Leverages Proven PKI Platform	VeriSign operates the largest and most comprehensive PKI solutions available on the market today, and has been doing so since 1995.

+ Learn More

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

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