



## DATA SHEET



### KEY BENEFITS

#### *24/7 Support*

Our support services consist of interactive online help and staffed services. VeriSign's customer support staff has the expertise in supporting more than 2 million individual and devices secured by certificates.

#### *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® Custom 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® Custom Device Certificate Service presents quick activation turnaround and an easy-to-use Web interface for certificate request and download.

## VeriSign® Custom Device Certificate Service and Certificate Key Ceremony Service

The need to authenticate hardware devices accessing networked services is on the rise as service providers continually strive to prevent unauthorized devices from gaining access to their protected networks and services. The WiMAX Forum™, formed in June of 2001 to promote the adoption of IEEE 802.16 compliant equipment by operators of broadband wireless access systems, is working to facilitate the deployment of broadband wireless networks by ensuring the highest security and interoperability of the corresponding broadband wireless equipments. Before WiMAX Forum Certified systems were available, every solution was custom and implemented in a proprietary authentication mechanism. WiMAX Forum Certified means a service provider can buy equipment from more than one company and be confident everything works securely together. WiMAX Forum Certified means a more competitive industry, lower costs, and faster growth for broadband wireless everywhere around the globe.

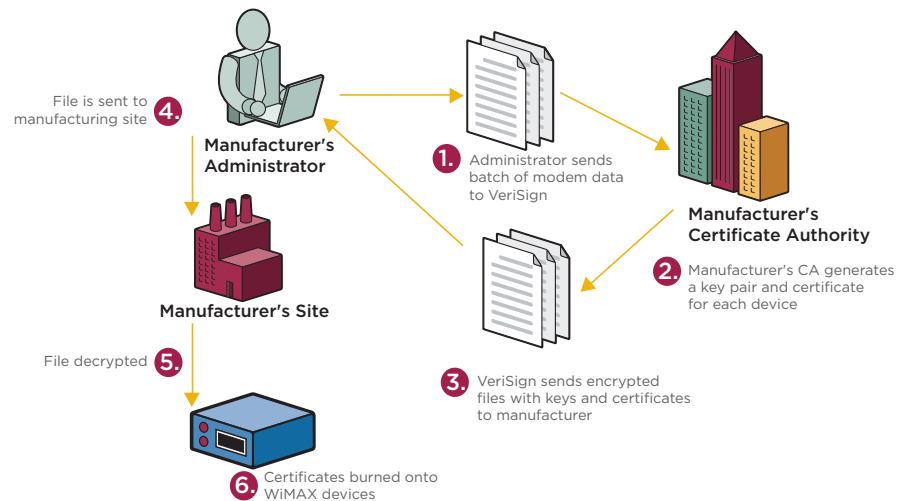
To establish the highest standard of wireless network authentication security, the WiMAX Forum requires that all WiMAX-compliant devices must be authenticated with X.509-standard digital certificates issued under the VeriSign managed WiMAX root Certificate Authority. Device manufacturers must comply with this security requirement to sell devices that are compatible with the WiMAX-standard system. Provisioning and managing digital certificates, however, requires a major investment and ongoing maintenance in security infrastructure. Instead of tackling that challenge yourself, turn to the digital certificate service experts at VeriSign.

### **+ VeriSign's Complete Turnkey Solution**

Take advantage of VeriSign's turnkey Custom Device Certificate Service to burn certificates and keys directly into your devices' circuitry. VeriSign's digital certificates fully comply with WiMAX Forums requirements and the 20-year certificate lifespan frees you from the obligation to process certificate renewals. The VeriSign® Custom Device Certificate Service is based on VeriSign's proven and scalable digital certificate architecture and is backed by 24/7 carrier-class managed services and guaranteed support levels. Keys and certificates are centrally generated and delivered securely in batches to mirror your manufacturing production runs.



Where it all comes together.™



### Device Certificate Request & Issuance Overview

With the VeriSign® Custom Device Certificate Service, device manufacturers order certificates in bulk by providing VeriSign with a list of MAC addresses and/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® Custom 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 Custom Device Certificate Service Web portal and upload a certificate request file (text format) containing the list of MAC addresses and/or serial numbers for the devices.
2. The VeriSign® Custom 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® Custom Device Certificate Service includes design and establishment of the CA structure for the right trust hierarchy. The VeriSign managed WiMAX 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 WiMAX root CA and can also host any sub-CAs issued under the WiMAX root CA 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.

### 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® Custom 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.

Note: At this time, WiMAX Forum does not require CRL certificate status checking on the 802.16d-standard CPEs (Customer Premise Equipments).

### + Certificate Key Ceremony Service

A manufacturer wishing to be WiMAX compliant, but that does not want to take advantage of VeriSign's turnkey Custom Device Certificate Service, may request that VeriSign sign a X.509-standard Certificate under the VeriSign-hosted WiMAX root CA at VeriSign's secure data center, and return the signed Certificate to the manufacturer. The signing of the Certificate(s) occurs during a VeriSign key ceremony.

### + Rely on VeriSign: the Digital Certificate Experts

VeriSign provides a simple way for device manufacturers to build devices equipped to prevent pirating through device cloning. By providing WiMAX compliant authenticated devices, you can not only offer customers the best secure service available, but also lay the foundation for accelerating the delivery of value-added services, including software delivery and content services.



## DATA SHEET

### + To Learn More

For more information about VeriSign Managed PKI, please call 650-426-5310, or visit [www.verisign.com/products/pki](http://www.verisign.com/products/pki).

**Visit us at [www.Verisign.com](http://www.Verisign.com) for more information.**

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. All other trademarks are the properties of their respective owners.

06-30-2006