



CASE STUDY



WildBlue Communications, Inc.

VeriSign Enables a Major Satellite Internet Service Provider to Further Promote Security and Affordability



WildBlue Communications, Inc.



SOLUTION SUMMARY

WildBlue Communications, Inc. wanted to keep the cost of its services and equipment affordable for subscribers while providing secure “last mile” communication and protecting itself against potential theft of service. WildBlue achieved this by leveraging DOCSIS/BPI+ standards and X.509 digital device certificates for device authentication. It turned to VeriSign for guidance and deployed VeriSign® Device Certificate Service. In three years 750,000 digital device certificates have been issued by the VeriSign-hosted CA to vendors producing satellite modems for WildBlue. WildBlue has been steadily growing its satellite broadband service offering while living up to its promise to provide a secure and affordable broadband service in virtually every corner of the continental U.S.

WildBlue Communications, Inc. is an Internet service provider that delivers reliable broadband connection via satellite for people in remote and rural areas requiring high-speed Internet connectivity. For consumers and businesses that do not have access to cable, DSL, or other high-speed broadband service options, WildBlue is one of the leading alternatives. According to the National Rural Telecommunications Cooperative (NRTC), there are close to 20 million U.S. households that simply would not have access to broadband Internet connectivity if it was not for services like WildBlue.

WildBlue utilizes two satellites to deliver its service. The first satellite was built and launched by Telesat of Canada in July 2004. WildBlue leases the U.S. payload on this satellite while Telesat uses other parts of the payload to serve the Canadian market. To meet the overwhelming demand for its service, WildBlue exclusively funded and launched the second satellite, named WildBlue-1, in December 2006 to serve the U.S. market. Both satellites employ leading-edge spot beam technology and were the first to deliver a commercial broadband service utilizing the Ka-band spectrum. The combination of Ka-band spectrum with spot beam architecture (that enables multifold spectrum re-use) differentiates WildBlue from its competition and allows it to provide higher bandwidth service tiers at an affordable price to virtually every household in the continental U.S., irrespective of geographical location.

+ Satellite Service Security

The satellite broadband business has some unique challenges due to multiple satellites that are using the same spectrum for transmission and being employed by multiple, and potentially competitive, service providers. Such a situation existed right at the start of service for WildBlue and Telesat subscribers living on the U.S.-Canada border. To ensure that WildBlue subscribers’ satellite modems only latch on to WildBlue’s service for its customers living along the U.S. side of the border with Canada, and not on to Telesat signals, WildBlue needed a way for modems to uniquely identify and latch on to the correct waveform. In essence, it required a modem to authenticate the service provider before deciding whether to establish communication with that network.

Aakash Sahai, senior director of access technologies for WildBlue Communications, Inc., recounted, “Back in 2000, we investigated many alternatives, some of which were suggested by our vendors, and discarded most of those as inadequate to address this rather unique service provider authentication requirement. We even considered the more conventional choice of provisioning every device with both Telesat and WildBlue reception capabilities so we could distinguish between them and redirect to each other’s network—this approach would have been expensive to manage and maintain. In the end we proposed, and co-developed with our equipment vendor, the Network Service Provider Authentication (NSPA) protocol based on X.509 certificates. VeriSign cryptography experts were helpful in reviewing the NSPA specification and validating that our NSPA concept would adequately address the requirements related to secure and reliable service authentication.”

Industry

- Telecommunications and Internet Services

Challenges

- WildBlue wanted to enhance security and integrity by leveraging open standards-based X.509 PKI digital certificates for device authentication.
- Needed to keep the cost of equipment and service attractive and affordable for rural subscribers.
- Had the operational requirement to restrict service registration by subscriber to WildBlue's network in the presence of other spatially-overlapping networks.

Solution

- VeriSign® Device Certificate Service

Results

- The VeriSign-hosted shared device manufacturers' CA has already issued 750,000 digital certificates for use in devices deployed in WildBlue's network.
- WildBlue is poised to make even larger gains in subscriber numbers.
- Cost-effectiveness of the VeriSign® public key infrastructure solution is one of the key contributing factors to maintaining low cost of equipment and service.
- Successful service coexistence with concurrent spatially-overlaid services operating in North America.

WildBlue opted to leverage the Data Over Cable Service Interface Specification (DOCSIS) standard that has been developed specifically for the cable industry. Under DOCSIS, digital device certificate authentication forces the validation of all modems requesting connection to a network.

DOCSIS' encryption provides appropriate data security across the complete transmission path, and its Baseline Privacy Interface Plus (BPI+) specifications require digital device certificate-based device authentication and public key cryptographic techniques to enable only authentic devices to connect to the network and securely exchange keys between modem and the hub equipment for data encryption. Digital device certificates that carry a modem's identity—its MAC (Media Access Control) address—are embedded in the modem and are signed using a chain of certificates. Each modem is assigned a unique MAC address and this address is used to identify a unique subscriber. X.509-based device-level authentication protects against situations where the MAC address in a modem has been tampered with in an attempt to gain unauthorized access to a service.

Sahai commented, "Setting up a secure and reliable Public Key Infrastructure (PKI) infrastructure to manage issuance of X.509 device certificates is non-trivial. VeriSign was already a market leader in managing PKIs for the cable industry, and we liked that it had already established the whole infrastructure to enable device manufacturers to request the device certificates in an efficient and secure way. It was an obvious choice for us to turn to VeriSign for help in setting up the PKI to serve our needs."

+ A Public Key Infrastructure Solution

VeriSign® Device Certificate Service is a high-volume, high-performance, batch issuance certificate service that provides a fast, efficient, and cost-effective way to embed X.509 PKI digital certificates into a wide variety of hardware devices during the manufacturing process. DOCSIS calls for embedding digital certificates in devices at the time of manufacture to provide nearly counterfeit-proof serial numbers. The manufacturer's Certification Authority (CA), or code verification certificate, must be signed under the proper root CA. For this purpose, VeriSign hosts the root Certification Authority and issues the PKI-based digital certificates, but will only sign digital certificates for those companies authorized to receive them. The DOCSIS root Certification Authority digital certificates are created for device manufacturers developing products or services that need to be authenticated. Embedding the digital certificate in the device or service enables applications to verify the validity of any DOCSIS-affiliated certificates by checking that they chain properly to the respective roots.

Sahai mentioned, "We did not want to take chances when it came to establishing the very infrastructure on which the security of our network and service would come to rely. While there were proposals by other vendors to host a low-cost PKI, we decided to partner with VeriSign to host and manage WildBlue's own Certificate Authority using the name BASIS (Broadband Access over Satellite Interoperability Specification) Root CA. Under BASIS Root CA we established the Shared Manufacturers CA from

“Leveraging the open security standard DOCSIS digital device certificate authentication mechanism has been much more cost-efficient to deploy than a proprietary security solution. By utilizing VeriSign Device Certificate Service, device manufacturers avoid a costly Certification Authority set-up. Our customers benefit because WildBlue’s equipment and services are far more attractively priced, and they can enjoy the same reliable secured communications that subscribers of DOCSIS-based cable broadband service have come to rely on.”

Aakash Sahai,
senior director of access technologies,
WildBlue Communications, Inc.

which the digital device certificates are issued for embedding into the satellite modems by our vendors. Using BASIS Root CA, WildBlue and Telesat also set up service provider CAs for issuing certificates that are embedded in satellite modems and the hub equipment to enable the NSPA functionality.”

+ Affordable Satellite Service is a Huge Success

In July 2005, WildBlue opened its satellite service and saw an immediate up-tick in subscribers. To date, the VeriSign-hosted shared manufacturers’ CA portal has issued 750,000 PKI-based digital certificates for devices. Stephanie Lovett, director of marketing at WildBlue, said “The demand for WildBlue’s service has been overwhelming. We continue to expect exceptional growth of service as we have established multi-year agreements with direct-to-home video-over-satellite providers DirecTV and EchoStar to offer WildBlue Internet service to their customers. In addition, WildBlue has an agreement with AT&T to deliver Internet services to AT&T subscribers that are situated in remote locations where AT&T cannot economically deploy cable or DSL. National Rural Telecommunications Cooperative members together account for another huge wholesale channel for WildBlue services and we have other nationwide partners that further augment our retail service offerings.”

“Utilizing DOCSIS and VeriSign Device Certificate Service has been very successful,” stated Sahai. “We’ve had no issues with digital device certificate issuance, and no problems operating side-by-side with Telesat along the U.S./Canadian border.”

The biggest benefit to leveraging a PKI-based solution has been felt by WildBlue’s customers. Sahai explained, “Leveraging the open security standard DOCSIS digital device certificate authentication mechanism has been much more cost-efficient to deploy than a proprietary security solution. By utilizing VeriSign Device Certificate Service, device manufacturers avoid a costly Certification Authority set-up. Our customers benefit because WildBlue’s equipment and services are far more attractively priced, and they can enjoy the same reliable secured communications that subscribers of DOCSIS-based cable broadband service have come to rely on.”

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

© 2009 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle, VeriSign Identity Protection and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and in foreign countries. All other trademarks are property of their respective owners.

00026851 02-18-2009