



## DATA SHEET



### VERISIGN AND TRUST-BASED SECURITY

From its inception, VeriSign has been a leading force in developing industry standards that define and govern trust-based security. Its early-stage participation in the creation of the broadly-adopted X.509 PKI standard is an example of this leadership in developing standards.

With the goal of making trust-based security ubiquitous, VeriSign has invested considerable time, effort, and resources in the development of the *VeriSign Trust Network* to enable global interoperability for PKI technologies. As a cornerstone of the *VeriSign Trust Network*, VeriSign's implementation of the X.509 standard (known as *Public Certificate Authorities*) has been embedded in all major Web browsers.

The behavior of Public Certificate Authorities is governed by VeriSign Authored *Certificate Policies*; which define roles, responsibilities, and usage for digital certificates; and *Certificate Practice Statements*, which define how a Certificate Policy will be implemented. The combination of Certificate Policies and Certificate Practice Statements enable the creation of a Public Certificate Authority, which serves as the basis for the VeriSign Trust Network. This *Public Certificate Authority*, and its components, clearly define how an organization can be compliant with VeriSign Trust Network, making it easier and more cost effective for organizations to implement trust-based security in their environment.

## VeriSign® Managed Public Key Infrastructure Service

As more transactions and correspondence are conducted electronically, there is an increasing need to authenticate users (i.e., “you are who you say you are”), restrict access to confidential information (i.e., “yield appropriate access to the right people”), and verify ownership of sensitive documents (i.e., “a piece of content has been authored and/or approved by a given individual”). Providing this level of trust-based security enables organizations to facilitate tighter integration with business partners, protect data against internal and external threats, ensure business continuity, and maintain compliance with government and corporate regulations. Security solutions based on Public Key Infrastructure, or PKI, are particularly well-suited in addressing these business needs.

PKI-based platforms allow a trusted Certification Authority (CA) to issue, renew, and revoke digital certificates for strong authentication, encryption, and for secure digital signing. Solutions based on PKI provide optimum value when they are:

- Cost-effective, both in terms of up-front cost and long-term total cost of ownership
- Reliable and based on a robust infrastructure of hardware, network, and software
- Scalable to meet ever-increasing business needs
- Supported by world-class professional services and customer support to ensure successful deployments
- Standards-based solutions that help preserve existing and future investments
- Based on well-established policies and procedures

### + VeriSign Managed PKI Service

VeriSign Managed PKI Service is a hosted solution that enables organizations to rapidly secure Web services, email, instant messaging, mobile workers, on-line forms exchange, legacy, and other applications. VeriSign's management and hosting of the PKI infrastructure enables a faster return on investment, a higher degree of responsiveness to meet evolving business strategies, and preservation of existing investments. Strong authentication (also known as “two-factor authentication”), digital signatures, and data encryption are core to the functionality offered by VeriSign Managed PKI Service.



**Enterprise End Users**—Using an Internet browser, subscribers are able to perform the following Managed PKI functions:

- Enroll for a new digital certificate
- Track the status of their application for a digital certificate
- Retrieve their digital certificate when it is issued
- Search for and verify another subscriber's digital certificate
- Renew their existing digital certificate
- Revoke their own digital certificate

**Administrators**—A Managed PKI administrator is authorized to review the requests for new IDs and renewals, and:

- Determine whether to approve or reject the requests
- Generate reports
- Search for account information
- Download Certificate Revocation Lists (CRLs) of digital certificates that have been suspended or revoked prior to expiration dates

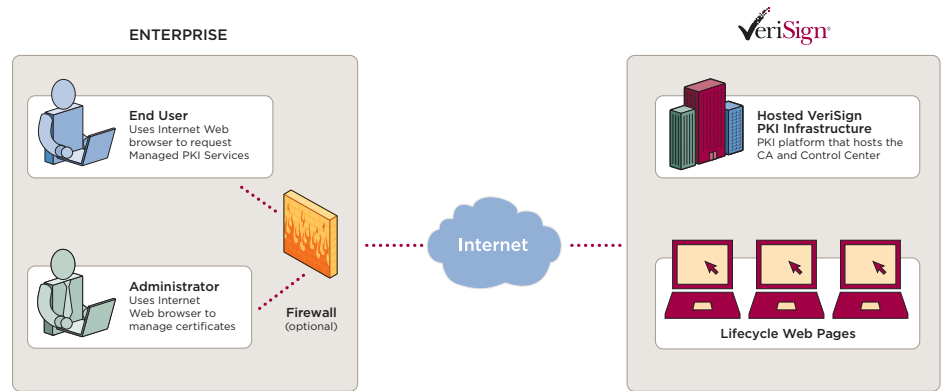
**VeriSign Issuing Center**—A hosted and managed PKI platform that:

- Processes requests for new digital certificates or renewals
- Processes the requests made by the end user and approved by the administrator
- Generates reports and CRLs, and uses Online Certificate Status Protocol (OCSP) standards to determine a digital certificate's status

By leveraging VeriSign's expertise and extensive PKI infrastructure, organizations spare themselves the expense and burden of building, deploying, and maintaining an in-house infrastructure while retaining complete control over certificate lifecycle management, including issuance, renewal, and revocation.

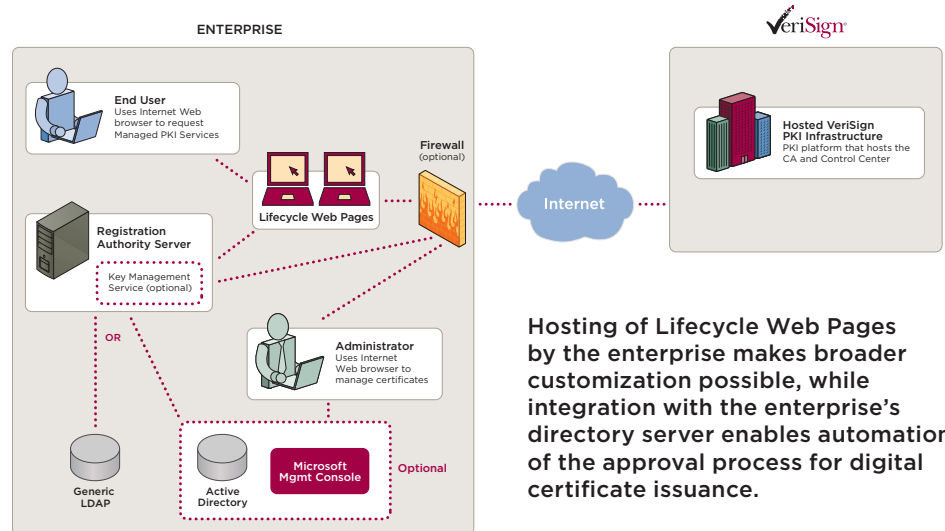
The following are distinct deployment options that an enterprise can choose when implementing VeriSign Managed PKI Service:

**Figure 1: VeriSign Managed PKI Service Fully-Hosted by VeriSign**



All PKI functions are hosted and managed by VeriSign, enabling the enterprise to focus on their core business.

**Figure 2: VeriSign Managed PKI Service Partially-Hosted by the Enterprise**



Hosting of Lifecycle Web Pages by the enterprise makes broader customization possible, while integration with the enterprise's directory server enables automation of the approval process for digital certificate issuance.

## + Features & Benefits

VeriSign Managed PKI Service provides day-to-day operation and maintenance of an organization's PKI environment, allowing in-house IT resources to focus on an enterprise's core business. VeriSign Managed PKI Service delivers the following:

<b>Hosted Certification Authority (CA)</b>	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"><li>• Generate Certification Authority key pairs.</li><li>• Activate and deactivate Certification Authority certificates.</li><li>• Maintain Certificate Revocation Lists (CRLs).</li><li>• Certificate issuance to internal and external users, Web servers and devices.</li><li>• Supports validation of a certificate's status using Online Certificate Status Protocol (OCSP) standards.</li></ul>
<b>Registration Authority (RA)</b>	Allow administrators to: <ul style="list-style-type: none"><li>• Authenticate, approve, or reject certificate requests from subscribers, and revoke certificates.</li><li>• Generate reports on certificate activity.</li></ul>
<b>Mission-Critical Reliability</b>	<ul style="list-style-type: none"><li>• VeriSign Managed PKI Service employs the same PKI technology that is used throughout its military-grade public key infrastructure and Network Operations Centers.</li><li>• Supports 24x7x365 monitoring, management, and escalation across the globe with full disaster recovery.</li><li>• Certified annually by KPMG as part of a SAS-70 security audit. A regular WebTrust audit of VeriSign's PKI infrastructure is also conducted.</li></ul>
<b>Complete Certificate Lifecycle Management</b>	Managed PKI Service Control Center gives enterprise administrators full control over enrolling, approving, revoking, and renewing digital certificates.
<b>Flexible Deployment</b>	<b>Fully-Hosted by VeriSign:</b> Solution is completely hosted by VeriSign at secure facilities. <b>Partially-Hosted by the Enterprise:</b> Enterprise may localize, brand, and host end-user enrollment pages.
<b>Automated Administration</b>	Interfaces with widely used directory services, such as Microsoft Active Directory, and automatically approves requests to issue or renew digital certificates.
<b>Scalable</b>	<ul style="list-style-type: none"><li>• Delivers carrier-class scalability, and is architected to support the highest volume and peak load requirements in the industry.</li><li>• Overall system architecture is designed to support the issuance and management of over 100 million certificates per year.</li><li>• VeriSign's diagnostic procedures, security practices, operational policies, and infrastructure have been tested and proven over time and designed with scalability in mind.</li></ul>
<b>World-class Service and Support</b>	<ul style="list-style-type: none"><li>• VeriSign's Professional and Support Services alleviate the burden of planning, implementing, and maintaining an in-house, full-scale support infrastructure.</li><li>• VeriSign Support Services can devote more resources to state-of-the-art technology, security, and training than is feasible for most enterprises.</li></ul>
<b>Rapid Deployment</b>	<ul style="list-style-type: none"><li>• In compliance with Public Certificate Authority specifications and VeriSign's existing infrastructure, the PKI platform, policies, and procedures are already in place and ready to be leveraged by customers.</li><li>• VeriSign Professional Services can implement an installation of VeriSign Managed PKI Service that is partially-hosted by the enterprise in less than one-third the time of a typical in-house, software-based PKI solution. With fully-hosted implementations, VeriSign manages the entire PKI environment on behalf of the customer.</li></ul>
<b>Standards-based</b>	VeriSign has a strong commitment to open standards, innovative technology, and strategic collaborations to enable the flexibility and ease-of-use that enterprises require. <ul style="list-style-type: none"><li>• Supports standard certificate types, including: S/MIME, SSL, and IPSec, as well as PKI industry standards such as X.509 v3, LDAP, PKCS #7, PKCS #10, and PKCS #12.</li><li>• VeriSign's open approach to security enables organizations to operate freely in diverse environments, and maximize return on, and preservation of, existing investments.</li></ul>
<b>Key Management Service</b>	Allows administrators to backup and recover user private keys with minimal risk and minimal security costs. This solution has three main functions: <ul style="list-style-type: none"><li>• Generate and distribute end user keys and digital certificates</li><li>• Backup of private encryption keys</li><li>• Recovery of keys and digital certificates</li></ul> The Key Management Service works with leading messaging solutions.
<b>Support for Third-party Hardware Security Modules</b>	Provides an added layer of security for solutions employing Local Hosting and Automated Administration.

## + Learn More

For more information about VeriSign Managed PKI Service, please call +61 3 9674 5555 or visit: [www.verisign.com.au/authentication](http://www.verisign.com.au/authentication)

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