



Certificate Revocation with VeriSign Managed PKI

Flexible, open revocation solutions for today's enterprise PKI needs



CONTENTS

Introduction	1
Today's Needs	1
Available Revocation Mechanisms	3
Certificate Revocation Lists (CRLs)	3
Partitioned CRLs	3
Online Certificate Status Protocol (OCSP)	3
Trusted Directories	4
Revocation Functions in VeriSign Managed PKI	4
Revoking a Certificate	4
CRLs	4
Managed PKI Validation Module for Web Servers	5
Online Status (OCSP)	5
Client-Side Revocation Checking	5
Summary	6
Open PKI—Best-of-Breed Applications	6
More Options	6
Lowest Total Cost	6
Real-world Non-Repudiation	6
Comparative Feature Support – VeriSign-Entrust	7

Introduction

In a public-key infrastructure (PKI), digital certificates, signed by certification authorities (CAs), are the means of distributing public keys accurately and reliably to users needing to encrypt messages or verify digital signatures. A certificate has a fixed lifetime, typically one year. However, a certificate may need to be revoked by a CA if a user private key is compromised or the CA is no longer willing to support the certification, for example, because the holder of the private key terminated employment with the enterprise. The PKI needs to provide applications that use certificates with the ability to check, at the time of usage, that the certificate is still valid.

VeriSign Managed PKI is VeriSign's unique integrated PKI platform.¹ Managed PKI combines enterprise-controlled and operated PKI software/hardware, an open PKI architecture giving compatibility with all popular applications, and the certificate processing services and infrastructure of a high-availability, high-security PKI backbone. The result is the most fully-featured, cost-effective, high-availability, and high-security PKI solution for the enterprise available in the world today.

Easy-to-use, readily deployable certificate revocation is an important enterprise PKI requirement, and VeriSign has built into Managed PKI the best in revocation technology. Revocation, however, depends as much upon the application software product as it does upon the infrastructure. Today's PKI-enabled products include varying degrees of support for certificate revocation.

Most of the application vendors participating in the Open PKI initiative² are responding rapidly to customer revocation/status-checking requirements that are emerging as PKI is being progressively deployed in mainstream business applications. As these applications expand their revocation/status-checking feature sets, VeriSign provides complementary functions on the infrastructure side.

This paper describes today's revocation needs, available techniques for revocation/status-checking, and VeriSign's current products/services and strategic directions relating to this aspect of PKI.

In today's fast-moving network security marketplace, it's important to ensure that today's PKI procurement decision won't become obsolete tomorrow. The breadth and depth of VeriSign's varied customer base and technical partners provides our enterprise customers the utmost confidence that their PKI investment will grow as their needs grow.

Today's Needs

Drawing on inputs gathered from over 120 VeriSign Managed PKI enterprise customers, plus prospective customers, affiliates, channel partners, and software vendor partners, and from the operational experience gained from issuing and managing millions of consumer and Website certificates, VeriSign has assembled a clear picture of revocation requirements in enterprise PKI today.

Revocation in enterprise PKI falls into two categories:

- **Server-side revocation checking:** A web server supporting SSL needs to check that a client certificate presented in an SSL handshake is valid, prior to granting access to resources on the basis of that certificate.
- **Client-side revocation checking:** A client using a certificate presented by a server or another client needs to check the validity of that certificate, e.g., for e-mail security purposes.

In the short term, server-side revocation checking is considered most important, and often indispensable, in order to close off access to web resources from credentials reported lost or compromised by customers or employees. Client-side revocation checking is also rapidly becoming an important requirement for some applications. Subsidiary requirements are:

- Revocation-checking must work with native-mode client software, i.e., it must not depend upon the installation of special client-side software. For example, server-side revocation checking must work with native browsers from the major browser vendors.
- It must be possible to revoke a certificate either manually by an administrator or automatically from enterprise administration systems or databases, e.g., automatically revoke an employee's certificate when the human resources database is updated to indicate that employee has terminated employment with the enterprise.
- While many applications can operate with latency of up to a day in a reported revocation becoming effective, other applications require much shorter latency and some require real-time status-checking.
- As a foundation for non-repudiation, records of revocation requests and notification postings must be retained securely under rigidly audited controls, and must be independently verifiable in the event of dispute resolution.
- Tools must be available to allow revocation status-checking to be integrated into any application in accordance with the principles of Open PKI (vendor independence).

VeriSign is committed to satisfying all of these requirements, in conjunction with our market-leading application partners. These requirements cannot be met with the standalone PKI software approach to building an enterprise PKI.

Available Revocation Mechanisms

Discussions with our leading partners and major customers have conclusively established that no single mechanism for certificate revocation will meet all needs. Risk management policy, trust models, timeliness requirements, population size and relationships between subscribers and relying parties create a variety of complementary mechanisms. Let us explain the mechanism options.

Certificate Revocation Lists (CRLs)

A certificate revocation list (CRL) is a digitally-signed, time-stamped black-list of revoked but unexpired certificates, issued by a CA periodically, e.g., daily. CRLs have the attractions of having a widely-recognized standard format (defined in the X.509 standard) and of being suitable for caching and use in non-online environments (e.g., when processing secure e-mail in a client which is not currently network-connected). They have limitations in that the CRL on hand may not be considered sufficiently fresh, and they may grow to an unacceptably large size.

Partitioned CRLs

To counter the problems of CRLs growing too large, there are various mechanisms of partitioning a CRL into smaller pieces. The CRL distribution point (CDP) mechanism defined in the X.509 standard provides for the population of users of a CA to be partitioned into fixed groups, with each group having its own CRL. A pointer in the certificate indicates the CRL partition (group) appropriate for that certificate. Application software follows this link to acquire the correct CRL partition. The group or link name is also included in the CRL and is used to confirm that this is the correct CRL for the certificate in question.

For greater flexibility in partitioning CRLs, VeriSign developed the Open CDP (OCDP) mechanism.³ Open CDP provides for CRL partitioning without fixed pointers in certificates.

Another mechanism defined in X.509 to help keep CRL sizes down is the delta CRL mechanism—a delta CRL contains only the latest revocation updates since a prior CRL was issued.

Online Certificate Status Protocol (OCSP)

Some applications—such as high value funds transfer—require immediate on-line checking of a certificate's status, rather than tolerate any latency as is inherent in all CRL-based mechanisms. An online mechanism is also ideally suited to integration of business processes that are inherently transaction oriented, automated clearing-house (ACH) transactions being a prime example. For such applications, the Internet Engineering Task Force (IETF) Public-Key Infrastructure X.509 (PKIX) Working Group developed the Online Certificate Status Protocol (OCSP) standard. OCSP species a transaction whereby a certificate-using application can obtain from a CA a digitally-signed indication of the current status of any certificate. While OCSP has excellent timeliness characteristics, it may present performance problems in comparison with CRLs, and is therefore not suitable for all applications.

Trusted Directories

For an intranet application, one approach to revoking certificates is to simply delete them from the enterprise directory. Such can be the case, for example, when an employee leaves a company—the employee's account is deleted from the system, including any digital certificates. To the extent that applications are designed to check for certificates in the directory prior to relying on them, this enables an expedient solution to the revocation requirement. This approach has its cost though: the directory now becomes a prime target of attack, and must be protected with comprehensive security controls. Furthermore, with inter-enterprise PKI, it may not be practical to make the trusted directory available to external relying parties to acquire the necessary account information for privacy reasons. Therefore, the trusted directory approach is of limited utility.

Revocation Functions in VeriSign Managed PKI

Revoking a Certificate

The VeriSign Managed PKI customer is always in control of the enterprise PKI. The Managed PKI Control Center provides an easy-to-use interface with which an administrator can:

- Revoke a subscriber's certificate;
- Query the status of current certificates;
- Manually download a CRL, produced nightly.

End users can also revoke their own certificates and query the current status of issued certificates.

In addition, the Automated Administration option of Managed PKI allows an enterprise to interface Managed PKI to a local administration system and revoke certificates automatically. For example, if Managed PKI is interfaced to the enterprise human resources database, an employee's certificate can be automatically revoked when the database is updated to indicate that the employee is about to terminate employment.

Enterprise PKI must support various revocation requirements of different applications. VeriSign generates CRLs daily or hourly for all enterprise customers. OCSP will also be supported for OCSP-enabled clients. In contrast, standalone PKI software vendors support only CRLs, usually only in conjunction with their proprietary client software.

CRLs

CRLs are generated by the VeriSign data center daily and made available for fetching by the enterprise. An option for hourly CRL issuance is also available with OnSite 4.0.

Managed PKI Validation Module for Web Servers

This Managed PKI module satisfies the requirement for server-side revocation checking. It features:

- A validation engine plug-in for Microsoft and Netscape Web Servers (IIS 4.0 and ES 3.5.1 or above, respectively) that enforces access control certificate revocation.
- Full configurability of CRL and CA certificate locations.
- An API providing application-level access to the validation engine's CRL maintenance, checking and automated retrieval functions.
- Automatic download of the Managed PKI daily or hourly CRLs.

VeriSign's Managed PKI Validation Module provides turnkey revocation status-checking for enterprise web servers that can operate with standard web browsers. In contrast, standalone PKI software vendors only implement revocation in conjunction with their proprietary client software products.

Online Status (OCSP)

VeriSign pioneered the development of real-time, automated status checking (OCSP). In the interests of industry-wide interoperability, we initiated and led the effort with the Internet Engineering Task Force (IETF) to establish OCSP as an industry standard. We were the first vendor to demonstrate OCSP operation in the 1998 National Automated Clearinghouse Association (NACHA) PKI trials and will provide OCSP support in conjunction with Netscape Communications Corporation's implementation of this protocol (as announced by Netscape in August, 1998).

Client-Side Revocation Checking

Client-side revocation checking functions depend largely upon the implementation choice of the client software vendor. VeriSign supports all the revocation mechanisms implemented by major vendors. For example, Microsoft has foreshadowed support for CRLs in forthcoming client product releases and Netscape has foreshadowed support for OCSP in its forthcoming releases. VeriSign Managed PKI will work with both as shipped—there is no need for troublesome proprietary client plug-ins as needed with PKI offerings of standalone PKI software vendors.

Furthermore, VeriSign supplies an application PKI-enablement toolkit that allows application implementors to easily incorporate CRL-based revocation checking into their applications.

Summary

Open PKI—Best-of-Breed Applications

VeriSign's strategy has been to partner with leading software vendors such as Microsoft, Netscape or Cisco in producing PKI-enabled applications. This allows us to focus on establishing and servicing the infrastructure that transforms commercial PKI into an integral component of everyday business processes. The software vendors—and others—are moving swiftly to expand their PKI offerings to address the concerns of their leading customers. Revocation is high on the list of "must-haves". The VeriSign customer has the widest possible set of deployment options, using industry leading PKI-enabled applications.

More Options

Some options—such as the trusted directory approach—are only useful in well-defined scenarios. CRLs, with or without the various CRL-partitioning mechanisms, show most promise for interoperability. Lastly, there will exist high-value, mission-critical applications that demand the immediate responsiveness and trust model flexibility that CRLs cannot provide. OCSP meets this need.

Lowest Total Cost

The VeriSign customer buys much more than software. VeriSign's integrated PKI platform solution represents an investment in physical structures, high-availability systems, off-site disaster recovery facilities and key management hardware and software that are benchmarks for the rest of the industry. We pioneered, developed and refined the commercialization of key management principles and processes which were previously only known to a select few within the Defense community. More important, however, are the skilled and knowledgeable staff that are required to operate these types of facilities and execute these highly trusted processes. These costs—frequently overlooked in software-only comparisons of PKI offerings—can make a massive difference for an enterprise considering a large, full-service operation.

Real-world Non-Repudiation

VeriSign Managed PKI supports non-repudiation in ways that are unattainable with fully enterprise-operated standalone PKI products. With Managed PKI, while the enterprise has full control over the issuance and revocation of digital certificates, complete records of the issuance and life cycle management of certificates are maintained by VeriSign in a high security, independently audited data center. Disaster recovery services operate around-the-clock at a geographically separated backup site. VeriSign's secure records are a readily available source of independent evidence that is available, if necessary, to facilitate speedy dispute resolution.

Comparative Feature Support – VeriSign-Entrust

VeriSign's features compare favorably with those of standalone PKI software product vendors. For example, Table 1 compares the VeriSign revocation features with those of Entrust.

Feature	VeriSign Managed PKI	Entrust
CRLs issued regularly	YES	YES
Server-side revocation checking, working with standard browsers	YES	NO
Automated revocation from enterprise administration system	YES	NO
Independently secured and verifiable revocation records to achieve non-repudiation	YES	NO
Disaster recovery	YES	NO
Online Certificate Status Protocol (OCSP)	YES	NO
Open PKI toolkit for enabling revocation in applications	YES	NO

For Further Information...

...see our website at www.verisign.com, contact your local VeriSign Account Representative, or call VeriSign at (650) 961-7500.

¹ For further details, see "Public-Key Infrastructure--The VeriSign Difference," VeriSign Strategy White Paper #98-01, 1998.

² See White Paper #98-01 for further details on Open PKI. Application vendors working on Open PKI initiatives with VeriSign include Microsoft, Netscape, and Lotus.

³ So named because this mechanism was developed originally as a free, "open" substitute for CDPs. The holder of the patent on CDPs was attempting, at the time, to levy license fees across the PKI industry for the use of CDPs. Two days after the publication of VeriSign's "Open CDP," the demands for license fees on CDP usage were withdrawn.