Oblix NetPoint Certificate Management Services

WHITEPAPER

FIRST EDITION

Printed in the United States of America.
Printing Date: July 2001

The purpose of this paper is to detail the benefits and technical description of Certificate Management Services functionality found within Oblix NetPoint. It should be noted that Oblix NetPoint offers full support of X.509 digital certificates as an authentication method for single sign-on. For more information on how authentication methods are applied with Oblix NetPoint or any other general architecture questions, please see Oblix NetPoint: A Technical Overview.

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
T 408.861.6800 • F 408.861.6810

European Headquarters
Regus House, Trinity Court
Wokingham Road, Bracknell
Berkshire RG42 1PL, UK
T +44(0)1344 668 014

www.oblix.com
info@oblix.com

Contents

Executive Summary 1

Oblix/VeriSign Certificate Lifecycle Management 2

Tighter Integration 2

Lower Total Cost of PKI Ownership 2

Certificate Management Services in Action:

An E-Business Scenario 3

Certificate Management Services Architecture 5

NetPoint Identity System 5

Identity Server 5

WebPass 5

Certificate Processing Server (CPS) 5

NetPoint Access System 6

IT Management Benefits 7

Built-In Local Registration Authority 7

Integration of Certificate Management with User and Enterprise Lifecycles 7

Flexible, Delegatable Workflow 7

Lower TCO 8

XML-Enablement of Certificate Information 8

End User Benefits 9

Single-Screen Identity and Certificate Management 9

Simple Renewal Process 9

Easy Access to Digital Certificate Public Keys 9

Single Sign-On 9

Conclusion 10

Glossary 11

Additional PKI Resources 11

Executive Summary

Enterprises are doing more business online. Along with increased Internet usage comes increased concern about the security of Web-enabled business resources shared with customers, business partners, employees, and contractors. Some business processes, applications, or systems require more protection than traditional username/password solutions. Where the risk warrants stronger protection in terms of authenticity, non-repudiation, and data integrity, enterprises have increasingly turned to using Public Key Infrastructure (PKI).

VeriSign is the world leader in PKI. It has been a pioneer in offering companies the ability to outsource portions of their PKI infrastructures for the following benefits:

- **Reduced complexity**. VeriSign simplifies the overall process of issuing, managing, and revoking certificates across multiple platforms and between enterprises and their users—a challenging process with many different components.
- **Greater manageability.** The complex, multifaceted process of certificate issuance, renewal, revocation, and lost key management can absorb in-house management expertise, time, and costs.
- **Lower total cost of ownership.** By outsourcing some PKI functions and leveraging VeriSign expertise, enterprises can reduce the cost of maintaining their PKI infrastructures.
- **Decreased liability.** When an enterprise acts as its own Certificate Authority liability is higher than if the certificate issuance is outsourced to VeriSign.
- **Built-in interoperability.** Enterprises want certificates that are globally recognized.

Analysts following the PKI market have pointed out the inherent benefits in the close integration of certificate management with identity management systems. In a June 2001 report entitled "PKI Vendors, Interoperability, and the Market," the Burton Group states that PKI vendors "need closer integration with identity management systems such as directory services, user provisioning systems, and access management systems."

"PKI vendors need closer integration with identity management systems such as directory services, user provisioning systems, and access management systems."

- Dan Blum
The Burton Group
June 2001

Oblix/VeriSign Certificate Lifecycle Management

Oblix NetPoint is a unified Internet security and management infrastructure that can be leveraged across all of an enterprise's e-business initiatives. This Web-access management solution delivers completely integrated Web single sign-on, policy-based authorization, and identity management.

An innovator in identity management solutions since its inception in 1996, Oblix has extended its expertise through a partnership with VeriSign, the world leader in PKI. Together they have examined the PKI challenges of infrastructure manageability, complexity, and usability and enabled Oblix NetPoint to seamlessly tie certificate management to business processes related to enterprise lifecycle events. This functionality is known as Certificate Management Services.

By building digital certificate management into the broader identity management process, the Oblix/VeriSign partnership has created benefits for end users and business managers alike. With a simpler certificate management experience, end users can go to just one place to manage their general identity information, including digital certificates and passwords. And enterprises can manage all facets of a user lifecycle more efficiently while tightening security management.

Tighter Integration

Certificate Management Services was built on the simple premise that security needs to be tightly integrated with enterprise business processes. With this certificate lifecycle management solution, an enterprise can:

- Limit complex infrastructure setup, maintenance, and liability via Verisign PKI that is pre-integrated with Oblix NetPoint
- Easily issue certificates to a multitude of users, both inside and outside its organization, at a low cost
- Eliminate security holes by automatically revoking certificates when a user should no longer have access
- Maintain flexible, low-cost certificate management via workflow-enabled processes that align with an enterprise's business rules
- Create a single coordinating hub for uniformly managing security policies enterprisewide via a variety of authentication schemes

Lower Total Cost of PKI Ownership

Many businesses want to minimize the cost of deploying and managing digital certificates, limit the risk entailed in issuing certificates, and reduce the expense of acquiring in-house certificate expertise. They increasingly are doing so by choosing to outsource PKI.

Market leader VeriSign has led the way in providing this support. VeriSign works with an enterprise's LDAP directory to handle certificate issuance, revocation, key recovery, and roaming services, among others.

Reducing certificate costs via outsourcing is only one means of lowering the total cost of PKI ownership. Consider these other cost factors that must be addressed.

- **Local Registration Authorities (LRAs)**. Setting up LRAs requires management expertise, labor, servers, centralized logging, and auditing.
- **Enrollment processes** (creating identities, assembling certificate enrollment information, seeking management approval). If not automated, enrollment processes result in high labor costs, especially if they are not integrated with enterprise entitlement and lifecycle processes such as employee hiring/termination, contractor management, business partner management, and access management.
- **Renewal and lost certificate processes**. Managing lost certificates and renewals can be costly not only in terms of money and labor but also in the time spent tracking down users, sorting out lost certificates, and waiting for access to applications and resources. Costs related to certificate loss and renewal are especially exorbitant when these processes are handled separately from other enterprise lifecycle events.
- **Revocation processes**. If certificate revocation processes are not tightly integrated with enterprise lifecycle processes, security can be easily breached—a costly weakness. Often worse than the hard costs associated with a security breach are the soft costs resulting from broken consumer trust and bad publicity. Help Desk professionals, certificate administrators, line managers, and users can also waste a lot of time trying to find out which certificates are valid and which ones aren't.

Let's take a closer look at how Oblix NetPoint and VeriSign together enable enterprises to successfully address these challenges of certificate manageability, usability, and complexity—while reducing total cost of PKI ownership. We'll examine the fictitious company Allied Industries, which selected NetPoint's rich functionality as part of its intranet and extranet authentication strategies. Following this scenario, we'll explore the underlying technical architecture of the integrated Oblix and VeriSign solution that enables its functionality.

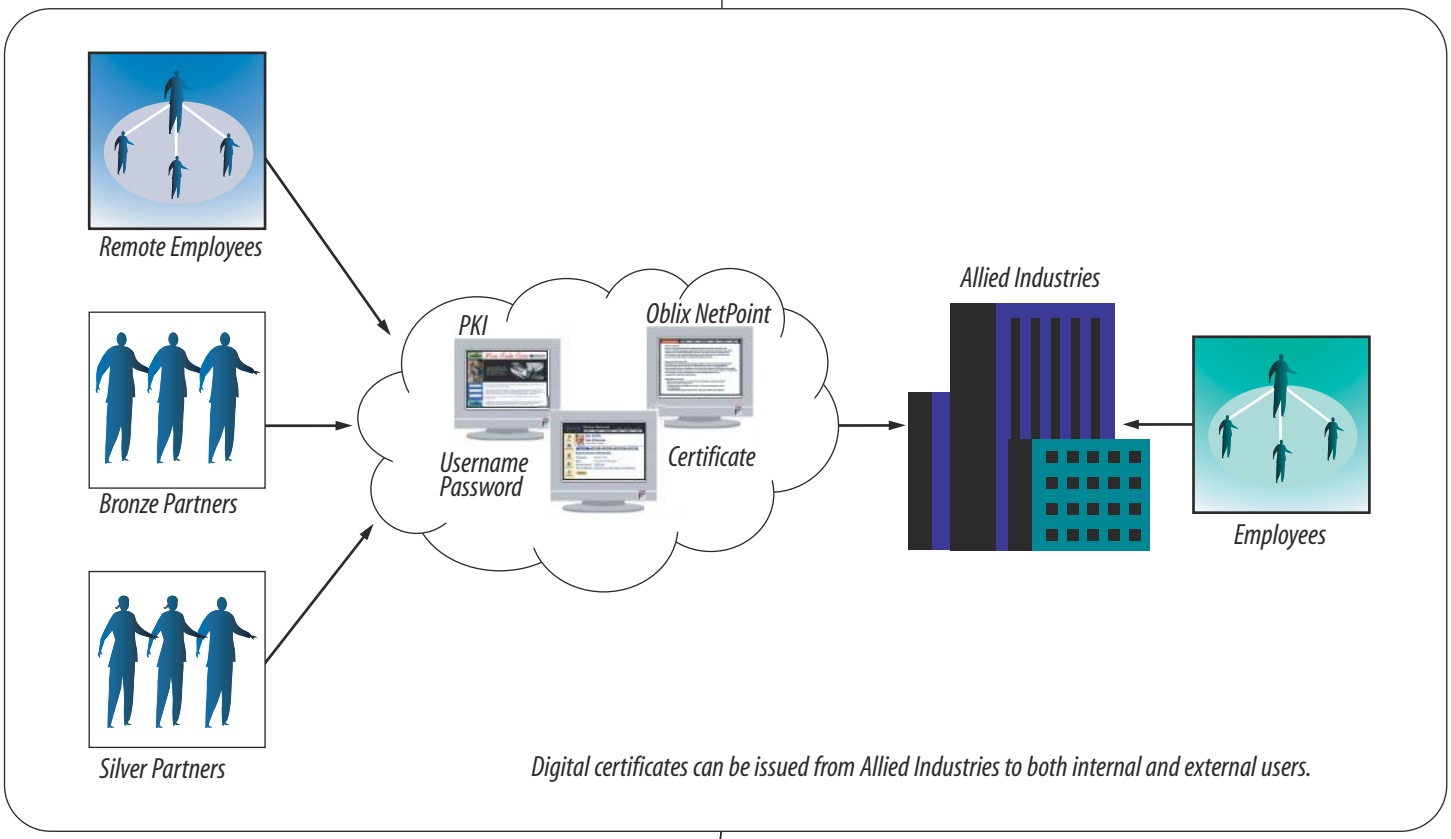
Certificate Management Services in Action: An E-Business Scenario

The manufacturer Allied Industries had an intranet for its employees and an extranet with its business partners. It wanted to use digital certificates to protect some of its most sensitive applications. Since each certificate issued would cost money to purchase and administer, Allied Industries began its careful planning by examining its intranet and extranet business processes to determine the correct approval processes needed for issuing, renewing, and revoking certificates.

For the intranet, Allied Industries decided that certain groups of employees—or those having certain job titles—should be automatically issued certificates with no required management approval. This included the executives with titles of VP or higher as well as groups within marketing that needed access to certain resources—such as sensitive sales and product information—that required security stronger than username/password protection. For the marketing users, Allied used Oblix NetPoint Certificate Management Services to automatically generate the information required to request a certificate from the LDAP directory. This streamlined the certificate issuance process, reducing the time and costs involved.

Allied Industries decided that other intranet users should have either one or two levels of management approval of their certificate requests, depending on the requester's title. For example, a contractor would require approval both from the person he or she reported to and from a manager. Employees would require only their managers' approval.

In both cases, Allied used the workflow features of NetPoint to issue certificate requests, to track and obtain manager approval, and to extract information needed for the certificate from the directory and the user (via a Web form). Once the information was approved within the company, it was then automatically sent via NetPoint to Allied's Certificate Authority, VeriSign.



Digital certificates can be issued from Allied Industries to both internal and external users.

Allied Industries decided it wanted to outsource the certificate authority to limit the certificate expertise it needed in-house, to limit its liability, and to take advantage of the experience of a world-trusted Certificate Authority (CA). It used VeriSign as its CA while acting as its own Local Registration Authority (LRA) via NetPoint. With this arrangement, Allied Industries could fully control and audit all the certificate-related activities through the NetPoint LRA and leverage VeriSign expertise. When a certificate was issued, it was automatically stored in Allied's LDAP directory, with notification sent to the requester.

For the extranet, Allied Industries divided its business partners into two categories: Silver and Bronze. Silver partners were those who conducted online transactions or passed back and forth sensitive information. Allied wanted a stronger security system than username/password protection for these users.

Allied Industries used the delegatable Certificate Management Services within NetPoint to allow its business partners to request and approve certificate enrollment themselves. It also used the workflow features of NetPoint to help the Silver partners handle their own certificate enrollment by entering some of the required information from the directory.

Most Bronze partners were allowed to continue to use the username/password system. Allied Industries retained the right to determine if a certificate would be needed for a Bronze partner accessing more sensitive applications or resources. It used the workflow features of NetPoint to have the business partners apply via the extranet to an Allied Industries administrator for certificate enrollment.

Enabling applications and resources requiring certificate authentication was also easy for Allied. Using NetPoint's out-of-the-box features, Allied Industries assigned applications and resources requiring higher levels of authentication a certificate scheme. This also neatly fit into Allied's single sign-on strategy, since NetPoint enabled it to maintain username/password authentication where it wanted to but to use PKI where higher security warranted it.

Allied Industries was also concerned about potential security breaches related to certificate revocation. Administrators had heard stories about users who had left a company or been transferred to a position in which they no longer needed access to certain protected applications—yet who still had access to those sensitive resources because the certificate revocation list had not been updated quickly enough. They also wanted assurance that all entitlement to applications or resources would be instantly denied when a user was terminated.

To handle this, Allied Industries took advantage of NetPoint Certificate Management Services. Each time a certificate was presented by the user at the beginning of a session, the certificate was automatically checked online via Oblix NetPoint. Further, when a user was terminated, NetPoint's integrated business processes automatically ensured that user access to all applications was terminated and that a revocation instantly occurred for the certificates the user held.

Allied Industries was also concerned about the usability of its certificates. It had heard of difficulties in users' renewing their own certificates, viewing which certificates they had, and finding the certificates of others. To solve these problems, it again called on NetPoint.

For example, Allied Industries wanted to spare users the frustration of having their certificates expire and consequently being denied access to applications. Allied Industries configured NetPoint to automatically place notes in the User Manager pages telling users to renew their certificates and to send escalating e-mails to both a user, his or her manager, and the Help Desk as the certificate expiration date neared. Allied also used NetPoint's simple point-and-click renewal buttons within the User Manager pages to save users effort and time.

Certificate Management Services were also used by Allied Industries to assist users trying to access other users' public keys in order to send encrypted e-mail. With the NetPoint Identity System functioning as a single, central location for all identity information, Allied users were able to quickly and efficiently search, find, and access the identity profiles of other users, where the public keys for their digital certificates were located. The public keys were then easily downloaded and made available for e-mail.

Allied Industries was pleased with its deployment of the integrated Oblix/VeriSign solution. It had reduced the total cost of PKI ownership, reduced certificate complexity, integrated PKI management into its business processes and systems, increased certificate usability, enhanced security following certificate revocation, and integrated certificate use into its single sign-on strategy.

Certificate Management Services Architecture

Oblix NetPoint provides a unified infrastructure security and management platform that can be leveraged by all of an enterprise's applications and users. Digital certificates can be managed through Certificate Management Services offered by NetPoint. Certificates are also used as an authentication method by the NetPoint Access System.

NetPoint Identity System

The Oblix NetPoint Identity System provides the interface through which IT administrators and end users alike manage all processes related to a user's identity lifecycle. This lifecycle can include creation of a user identity profile, management of usernames and passwords, certificate requests, distribution and revocation, and user deactivation.

The NetPoint Identity System includes the following components.

Identity Server
The Identity Server is an installable, standalone server that processes all requests for managing user identity, group, organization, and credential information (such as certificates and passwords). Organizations can set up multiple instances of the server if necessary.

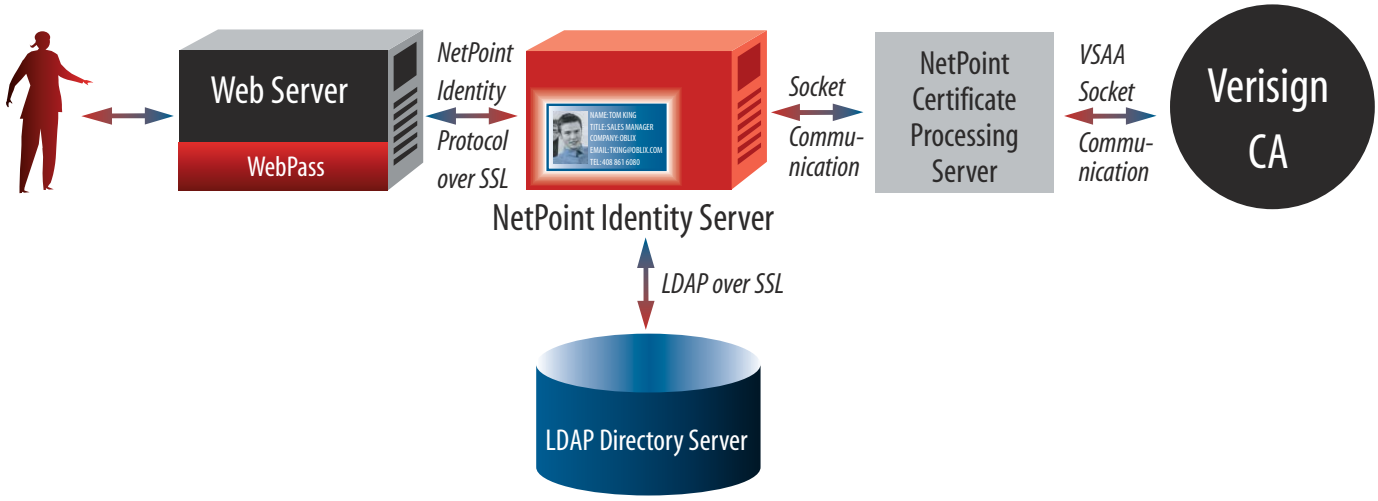
WebPass
The WebPass component of the NetPoint Identity System is a plug-in placed on the Web server to pass information back and forth between the Web server and the Identity Server. This three-tier architecture enables an organization to host the Identity Server behind its server firewall and outside its DMZ. This capability delivers improved security since the LDAP directory server is not exposed outside the firewall.

Certificate Processing Server (CPS)
This component serves as an LRA (local registration authority) enabling requests coming from the Identity Server to be communicated to the VeriSign CA Processing Center. The CPS is based on technology Oblix has licensed from VeriSign and then further enhanced with identity management functionality.

The following example illustrates how a typical request for a digital certificate flows from the user to Oblix NetPoint to the VeriSign certificate authority and back.

1. A user accesses the NetPoint Identity System to manage information regarding her personal identity profile.

2. Through the User Manager in the NetPoint Identity System, she accesses her "My Identity" page that includes the certificate lifecycle management functionality.



Certificate Management Services is integrated within the broader user identity lifecycle.

3. If she has been given the right to request a certificate, she will see a button that enables her to begin a certificate request. The browser transparently sends her request to WebPass.

4. WebPass passes the http(s) request to the Identity Server.

5. The Identity Server communicates with the Certificate Processing Server (CPS) via a secured socket connection. The CPS acts as the Local Registration Authority.

6. A secured socket connection is then made from the CPS to the VeriSign Certificate Authority (CA) in the VeriSign Processing Center.

7. The VeriSign CA then approves the request and generates a digital certificate, which is then transferred back to the NetPoint CPS.

8. The CPS then transfers the digital certificate back to the NetPoint Identity Server, which places the digital certificate in the LDAP directory.

9. The Identity Server then returns a call to the user's browser telling her the certificate has been issued.

This general process for certificate issuance applies to certificate renewal and revocation as well.

For online certificate status checking, Oblix NetPoint works seamlessly with VeriSign via the Online Certificate Status Protocol (OCSP). Using this feature, Oblix NetPoint instantly verifies certificate validity for each user session during which a certificate is presented for use in authentication.

NetPoint Access System

Common security for multiple Web and non-Web resources and applications is managed via the NetPoint Access System, which is highly integrated with the NetPoint Identity System. The NetPoint Access System is a complete solution that ensures that only authorized users can gain access to information, applications, and resources residing across virtual organizations.

Protecting resources with the NetPoint Access System allows an enterprise to PKI-enable its applications. Enterprises can set up a policy that requires a user to authenticate with a digital certificate. The NetPoint Access System accepts X.509 digital certificates.

IT Management Benefits

As companies look to deploy PKI more quickly and with fixed budgets, they look more closely at outsourcing PKI. VeriSign is the clear market leader for this approach.

Oblix NetPoint Certificate Management Services, designed to interoperate with VeriSign technology, enables IT managers to simplify and streamline certificate management within business processes. Once an IT manager has structured an agreement with VeriSign to purchase certificates and activate a company account, the rest of the PKI setup is built into Oblix NetPoint.

First, the IT Manager sets up the Certificate Processing Server (CPS) within Oblix NetPoint to serve as a Local Registration Authority (LRA). Once established, the CPS then works with the logic in the NetPoint Identity System as the central hub for administering certificate management business processes that fit the company's needs. The following IT benefits result from this integrated certificate lifecycle management.

Built-In Local Registration Authority

Because the LRA is installed as part of the Oblix NetPoint installation, deployment and setup time is minimized. And because the CPS works seamlessly with VeriSign and supports OCSP—which is a protocol used to check the status of certificates—less effort is needed for additional setup and configuration.

Additionally, IT managers greatly benefit from VeriSign outsourcing. There is no need to invest in establishing a local Certificate Authority (CA) since those functions are all handled by VeriSign.

Integration of Certificate Management with User and Enterprise Lifecycles

Oblix NetPoint gives IT managers the ability to link certificate enrollment, renewal, and revocation processes with enterprise lifecycle events such as employee hiring/termination, contractor hiring/termination, promotions, and transfers.

Just as in the Allied Industries scenario, IT managers at every company need to think through the proper requirements for certificate enrollment, renewal, and revocation. This includes determining which people in which roles or positions require authorization for certificate requests and changes as well as how information for each certificate enrollment is to be assembled. Lower management and labor costs can be achieved if required information is automatically filled in from the enterprise's LDAP directories.

The IT manager sets up the workflow within NetPoint for certificate enrollment, renewal, or revocation to route requests to one or more levels. This is usually done using groups, roles, positions, titles, specific individuals, or combinations thereof that can be found in the directory. The setup time is minimal once the business process is outlined.

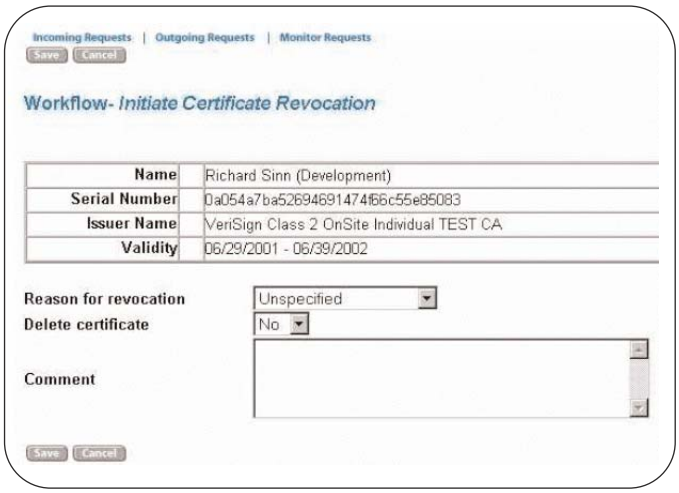
In a typical enterprise, the Human Resource Management System (HRMS) is the authoritative source for determining an employee's professional information, such as status and job title. If NetPoint Certificate Management Services is merged within the broader user lifecycle, a change in the HRMS can trigger a change in the directory. The NetPoint Identity System then can pick up the change in the directory and apply the rule the IT manager has set. This might mean that a certificate is issued to a user who will need one in his or her new role, or that a certificate is revoked in response to an employee termination.

It's important to note that delegation and approval of certificate enrollment can extend outside an enterprise as well. As in the Allied Industries example, an IT manager using the Identity and Access Systems within Oblix NetPoint can delegate portions of the enrollment to business partners. This helps allocate certificate costs as close to the user as possible and offload enterprise IT labor costs that would be otherwise spent in managing the process.

Flexible, Delegatable Workflow

Oblix NetPoint comes equipped with a built-in workflow engine that can be used to automate user requests and approvals. IT managers can use the multi-step, delegatable workflow features to tailor certificate management to business processes. For example, in the case of a job termination, the workflow might be to revoke a user's certificate and block all further access to all applications and resources.

Such a request would be passed to the CPS, which in turn would request the revocation from VeriSign. A few seconds later, the employee's certificate would be revoked. At the same time, the NetPoint Access System would terminate access to all applications and resources regardless of authentication method. The result: lower management costs with little or no labor required for processing and notification, immediate response, and higher security.



To set up a workflow-enabled revocation process, a NetPoint Administrator would take the following steps:

1. The administrator would sign on to NetPoint User Manager to access the Revoke button, if he had been given the rights to do so.

2. Optional user-entered information plus information from the LDAP directory would be combined to complete the certificate revocation. For example, through a NetPoint workflow step the administrator might be requested to enter the reason of revocation. This specified reason would be stored in a NetPoint configuration file and used later, for example during an audit, to reveal the purpose of the revocation.

3. NetPoint would then follow the revocation workflow, according to the required steps previously defined by the enterprise: notifications to other people, information entry, approvals, etc. The revocation process can be simple or have multiple steps.

4. Once the revocation process was completed, the information would be sent to the CPS, which would then send it to the VeriSign CA for processing.

5. The VeriSign CA would give the revocation result to the NetPoint CPS to confirm that the revocation had been successful. (A retry or notification to administrator(s) can be set up when revocation fails.)

6. The status of the certificate would be changed to REVOKE in real time as OCSP is used for status checking.

7. The certificate could then remain in or be deleted from the LDAP directory. If an enterprise chooses to delete revoked certificates, this process can be automated through Oblix NetPoint.

Low TCO

Total cost of ownership is lowered by reducing labor costs associated with PKI management, integrating certificate management with business processes, and integrating certificate security with centrally managed authentication policies.

As noted earlier, Certificate Management Services can substantially cut expenses related to certificate enrollment, renewal, loss, and revocation management. Oblix NetPoint's multi-step delegatable certificate management workflow process, linked to the NetPoint Identity System, means formerly separate business processes can be integrated and automated wherever feasible.

Integrating certificates into the central enterprise authentication and authorization hub provided by NetPoint further reduces the labor and time dedicated to ensuring the right authentication scheme is applied to the right application and resource by the right person.

By relying on the VeriSign services integrated with Oblix NetPoint and on the built-in LRA, companies can eliminate the need for expensive in-house certificate expertise. In addition to labor savings and limited liability, the enterprise also gains from VeriSign's globally recognized certificates.

XML-Enablement of Certificate Information

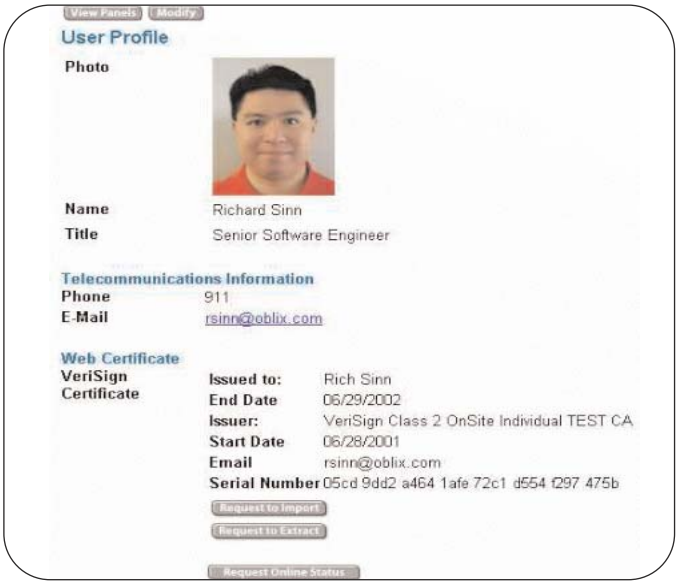
Enterprises are increasingly using XML to more efficiently exchange data between their systems. IT managers looking to leverage the benefits of XML can configure NetPoint to provide XML output of digital certificate information. This output can then be accessed by other systems that require XML input about digital certificates. Additionally, this XML output can include user identity profile information beyond digital certificate information. This capability gives management greater flexibility in exchanging identity, security, and directory data amongst applications.

End User benefits

End users also realize the following significant benefits when using Certificate Management Services within Oblix NetPoint for certificate lifecycle management.

Single-Screen Identity and Certificate Management

Users have just one place to go to locate their enterprise identity information: the NetPoint Identity System. It's built into the intranet, extranet, or Internet pages of the enterprise. Via the easy point-and-click NetPoint User Manager, a user can view and/or manage his contact information, the certificates he has, and the applications he's entitled to use. From the same User Manager Web pages, he can also determine when his certificates will expire and how to apply for a certificate.



For example, when a user applies for a new certificate, the enrollment process set up by IT management is automatically enforced. This workflow enrollment process checks to see if the user should be allowed to request a certificate, thus restricting certificate requests only to appropriate users.

The process can be as streamlined as the IT system manager deems appropriate. Much of the information required in the certificate may be automatically retrieved, if available from the enterprise LDAP directory, and placed in the form the user sees on-screen.

Alternatively, users may be required to fill in portions of the information with the rest of the information to be filled in by their managers. When a certificate has been approved by the VeriSign Certificate Authority (which receives the request from the NetPoint CPS and sends the approval back to the CPS), the user receives a notice in User Manager.

Simple Renewal Process

Users whose certificates are about to expire are also notified. The notification process is configurable by IT management, and can either be done through the NetPoint User Manager user interface, or by e-mail.

The notification can consist of automatic e-mail notices triggered to be sent at a prearranged time before the certificate expires. Notices in the User Manager may also alert the user to the fact the certificate will expire. Optionally, management may also decide to automatically notify the user's manager or the Help Desk.

Easy Access to Digital Certificate Public Keys

Users can also easily find and use the public certificates of other users. For example, if Mary wants to encrypt an e-mail to Jane Smith, but doesn't have Jane's public certificate, here's what she would do.

1. Access the NetPoint identity search function.

2. Using the drop-down menus, enter the user's name: Jane Smith.

3. Select the user, "Jane Smith," from the resulting screen display and click on the certificate displayed in Jane's identity information.

4. Download Jane's public certificate and use it to encrypt the e-mail using the e-mail program.

Single Sign-On

Both internal and external users benefit from Oblix NetPoint's rich single sign-on features. It reduces the number of authentication mechanisms needed to access applications and resources as well as the number of times authentication is required. For example, users may access all applications and resources that share the same authentication requirements by presenting the requisite certificate only once.

If a user without a certificate tries to access a resource or application that requires a certificate, Oblix NetPoint can be configured to redirect him to a Web page allowing him to apply for certificate issuance. He may also be directed to his manager or to a Help Desk if authentication rules do not permit him to request a certificate. This is automated through Oblix NetPoint without custom programming.

Conclusion

The ability to integrate PKI with business processes related to normal enterprise and user lifecycle events is critical. Oblix and VeriSign have partnered to provide integrated certificate lifecycle management in a manner not available from other vendors.

The resulting solution, NetPoint Certificate Management Services, is the first to seamlessly integrate certificate lifecycle management within a broader user identity management system.

Through Certificate Management Services, enterprises can implement PKI with

- low cost,
- low complexity,
- high business process integration,
- enhanced security, and
- greater usability.

PKI becomes a manageable, scalable security solution with a low total cost of ownership. By issuing, revoking, and renewing certificates in conjunction with user lifecycle changes, enterprises can eliminate security holes and operate more efficiently. They can also take full advantage of NetPoint's unique capability to offer customizable workflows for these processes and to delegate approval responsibility.

With Certificate Management Services, these companies can meet the PKI challenge reliably and cost-effectively for maximum infrastructure security and manageability.

Glossary

- ACCESS SERVER. A server within the NetPoint Access System that enforces enterprise authentication, authorization, and auditing functions.

- CERTIFICATE AUTHORITY(CA). The authoritative source for issuing certificates. VeriSign acts as the Certificate Authority for issuing VeriSign digital certificates.

- CERTIFICATE PROCESSING SERVER (CPS). The local registration authority (LRA) within Oblix NetPoint. The NetPoint CPS is based on technology Oblix has licensed from VeriSign and then further enhanced with identity management functionality.

- IDENTITY SERVER. An installable, standalone server within Oblix NetPoint that processes all requests for user identity, group, organization, and credentials management. Organizations can set up multiple instances of the Identity Server if necessary.

- LOCAL REGISTRATION AUTHORITY (LRA). The authority for managing certificate enrollment, storage, distribution, and renewal processes and for requesting certificate issuance and revocation services from the CA. In Oblix NetPoint, the Certificate Processing Server (CPS) is the LRA.

- NETPOINT IDENTITY SYSTEM. The system through which IT administrators and end users alike manage all processes relating to a user's identity lifecycle. This lifecycle can include creation of a user identity profile, management of usernames and passwords, certificate requests, distribution and revocation, and user deactivation.

- ONLINE CERTIFICATE STATUS PROTOCOL (OCSP). A protocol that allows for real-time checking of certificate revocation status via a secured Internet connection.

- WEBPASS. A NetPoint plug-in placed on the Web server to pass information back and forth between the Web server and the Identity Server.

For more VeriSign and PKI related definitions, visit
http://www.verisign.com/repository/CPS/CPSCH13.HTM

Additional PKI Resources

Burke, Brian, Chris Christiansen, and Charles Kolodgy. Worldwide Security 3As Software Market Forecast and Analysis, 2000-2004, Authentication, Authorization, and Administration Accelerate eBusiness Enablement. Framingham, MA:
IDC, March 2001.

PKI Market Magic Quadrant 2H01. Stamford, Conn.:
Gartner Research, April 23, 2001.

Public Key Infrastucture Vendors, Interoperability and the Market:
The Burton Group, June 20,2001

The Second PKI Hype Cycle. Stamford Conn.:
Gartner Research, February 22, 2001.

Thompson, David. The Reality of Public Key Infrastructure Technologies. Stamford, Conn.:
META Group Inc., August 2, 2000.

Wheatman, Victor. Threads: The Killer Application for PKI? . . . All of the Above. Stamford, Conn.:
Gartner Research, June 8, 2001.