



WHITE PAPER

VeriSign Unified Authentication

The Next Generation of Strong Authentication





WHITE PAPER

CONTENTS

+ Introduction	3
+ The Need for Strong Authentication	3
+ Barriers to Adoption	4
Lack of Interoperability	4
Poor Integration	4
Costly Hardware and Infrastructure	4
Lack of Scalability	5
+ Introducing Unified Authentication	5
+ The VeriSign® Unified Authentication Solution: Value, Flexibility, Longevity	6
Single Platform, Multiple Credentials	6
Multipurpose Next-Generation Tokens	6
Deployment Flexibility and Scalability	6
+ Solution Components and Architecture	7
Strong Credentials	7
Validation Services	9
Provisioning and Lifecycle Services	10
Self-Service Applications	11
Management Services	12
Application Integration	13
+ Solution Scenarios	14
Secure Remote Access	14
Banking Web Application	15
Token Coexistence	16
+ Conclusion	17
VeriSign Unified Authentication Solution: Key Differentiators	17
+ For More Information	18



Where it all comes together.™

VeriSign Unified Authentication

The Next Generation of Strong Authentication

+ Introduction

The expansion of enterprise networks, an increasingly mobile workforce, and the need to bolster consumer confidence in online security are driving organizations to adopt strong, two-factor authentication mechanisms to ensure that only legitimate users have access to sensitive information and transactions. Strong authentication has become especially critical as network attacks and data theft become more sophisticated, enterprises open their networks to include suppliers, customers, and business partners, and regulatory-compliance requirements become stronger and more pervasive. Even so, the expense and complexity of strong-authentication solutions frequently impedes their adoption. Poor interoperability, a profusion of devices, and security-infrastructure implementation and maintenance all contribute to complexity and cost.

To address these issues, VeriSign has introduced a new solution for strong authentication. Based on the open-authentication road map promoted by the Open AuTHentication (OATH) working group, the VeriSign® Unified Authentication solution provides a common, open standards-based platform for authenticating users and devices. Using the highly scalable solution, enterprises can deploy multipurpose credentials that support Windows® log-on, virtual private networks (VPNs), Wi-Fi roaming, and application security in both plugged and unplugged mode.

The solution reduces total cost of ownership (TCO) of strong authentication by as much as 40 percent by leveraging an enterprise's existing infrastructure, employing cost-effective tokens, enabling self-service management of common certificate-lifecycle tasks, and offloading security, service, and scalability requirements to VeriSign. As a key component of VeriSign's Intelligence and Control Services, Unified Authentication gives financial institutions, government agencies, health-care organizations, and retailers an unprecedented level of control over their IT environment, enabling them to proactively pursue new opportunities in commerce and communications—while mitigating today's cost, complexity, and compliance challenges.

+ The Need for Strong Authentication

Even as innovative business models and impressive advances in technology fuel industry's vision of the Internet as a dynamic medium for commerce and communication, security issues continue to weaken confidence in online business. One of the most vexing and serious security issues is related to identity verification. If users and devices accessing the network are not properly identified, enterprises risk exposure to threats like fraud, phishing, identity theft, IP spoofing, and denial-of-service attacks. The problem is compounded as information becomes accessible through myriad devices and channels, each with its own security mechanisms, protocols, and proprietary technologies. A user today, for example, can access email via his or her office desktop, wireless laptop, pager, or cell phone, or even via a cyber-café kiosk.

Strong, two-factor authentication addresses the need for advanced levels of identity verification and is essential for preserving confidence in online commerce and communication. By requiring users to present something they know (such as a user name/password or a personal-identification number, or PIN) with something they have (like a token or a digital certificate/smart card), strong authentication helps prevent identity theft, allows enterprises to open their networks to suppliers, customers, and business partners, and protects user devices and Web services. These capabilities, in turn, foster the creation of trusted networks, where enterprises can allow new business opportunities and strategic partnerships to ripen, increase the yield on existing investments, and more fully leverage high-value services such as voice over IP (VoIP), online supply-chain management, electronic content exchange, and e-commerce.

PHISHING EXPLOITS ON THE RISE

Phishing is a form of social engineering in which criminals pose as legitimate entities in order to obtain personal information such as credit card numbers, account passwords, and Social Security numbers from unsuspecting consumers. Typically, phishers use fraudulent Web sites or the email addresses of trusted brands in order to send spam email messages that dupe recipients into providing confidential data. They then use the personal information to commit credit card fraud, identity theft, and other crimes.

Unfortunately, phishing attacks continue to rise at an alarming rate. According to the Anti-Phishing Working Group, the average monthly growth rate in phishing attacks, through July 2004, was 50 percent. In its report "Phishing Attack Trends," the industry working group indicated that financial institutions had been the most heavily targeted, with retailers following. In addition, although the United States was the source of 35 percent of all phishing exploits in July, South Korea, China, Taiwan, Russia, the United Kingdom, and Mexico also hosted a significant number of phishing sites. Strong authentication helps combat phishing by enabling organizations and consumers to more reliably verify the identity of email senders, Web sites, devices, and other users.

+ Barriers to Adoption

In today's enterprises, IT groups have to address the diverse authentication needs of many user constituencies, including system administrators, employees, business partners, and customers. For example, system administrators may require a hardened public key infrastructure (PKI) solution, where keys and certificates are protected by a USB smart card. Employees who want to combine physical-access security with strong network authentication may require a smart card aggregating use of a one-time password (OTP), PKI, and building-access credentials. External users such as remote VPN users, business partners, and customers may prefer the simplicity of clientless OTP tokens. Users who conduct high-value transactions and need nonrepudiation capabilities may require a hybrid authentication platform that can combine OTP and PKI functionality. Finally, enterprises rolling out large-scale consumer applications may favor consumer scratch cards over more costly electronic devices for authentication.

Existing strong-authentication methods are veritable point solutions that do not adequately address the totality of these requirements. They often favor a specific device (such as a smart card, OTP token, or PKI token) and authentication mechanism (OTP or PKI) over another. And although they resolve problems related to identity verification, their complexity and high cost of ownership create artificial barriers to adoption. Lack of interoperability, poor integration, hardware and infrastructure costs, and lack of scalability are key impediments.

- **Lack of interoperability** – To accommodate diverse usage scenarios, enterprises frequently deploy multiple proprietary authentication mechanisms. Because these closed solutions rely on proprietary hardware, protocols, and middleware, they do not interoperate easily with the products of other vendors. This lack of interoperability prevents deployment of cost-effective, best-of-breed solutions. In addition, tightly coupled, proprietary components impede migration to more advanced solutions; a single element cannot be replaced without replacing the entire solution. This limitation forces enterprises to depend heavily on a single vendor that has no incentive to reduce cost or drive innovation over time.
- **Poor integration** – Strong authentication solutions that rely on proprietary technology are difficult to integrate with other applications or devices. This limitation forces enterprises to rely on separate authentication solutions for each method of authentication across applications (such as OTPs, X.509 certificates, and smart access cards). Proprietary solutions also tend to introduce separate and heavy infrastructure components instead of integrating into the existing identity-management fabric. For example, they may require separate servers with duplicated user data instead of tightly integrating with core network infrastructure such as corporate or user directories. This requirement in turn compounds the complexity of managing credentials and users because the strong-authentication capabilities must reside outside the traditional identity-management infrastructure (such as provisioning, administration portals, and directory servers).
- **Costly hardware and infrastructure** – Strong-authentication solutions traditionally rely on specialized security hardware (such as tokens and smart cards). Because these devices are not interchangeable, vendors can command artificially high prices. Lack of interoperability, costly application integration, and the absence of unified management capabilities all add up to make today's solutions very expensive. In addition, implementing, managing, and maintaining an always-on strong-authentication infrastructure requires significant time and resources. Many enterprises lack the security expertise and resources to deploy reliable OTP, PKI, or smart-card solutions in house.

OATH:

A New Vision for Universal Strong Authentication

The initiative for Open AuTHentication (OATH) is a collaboration among hardware credential providers (ActivCard®, Aladdin Knowledge Systems®, ARM®, Axalto®, Gemplus®, Rainbow Technologies®, and Authenex®) to create a common standards-based platform for managing both standalone hardware credentials such as those for smart cards and tokens and embedded hardware credentials like those for cell phones, personal digital assistants (PDAs), and laptops.

OATH has created a road map for the collaborative development of an open strong-authentication specification that can be adopted across the industry. The road map, which emphasizes the use of existing technology and open standards, is intended to provide a starting point for designing an open architecture.

The resulting open architecture will provide the foundation for interoperable solutions that can be deployed across devices, identity-management platforms, and networks while allowing innovation that brings new products to market.

OATH has been endorsed by leading network and application providers including BEA Systems®, Check Point®, Cisco Systems®, Entrust®, Hewlett-Packard®, IBM®, and Sun Microsystems®.

- **Lack of scalability** – Most of today's solutions are standalone, requiring user data to be replicated across devices and networks. Data replication requires tremendous computing power to cope with the large number of users, as well as custom software to integrate authentication mechanisms into business applications. Managing multiple devices and creating the infrastructure to support high performance, global availability, and rapid growth of data directories is a complex, time-consuming, and costly task.

+ Introducing VeriSign Unified Authentication

To accommodate a broad range of applications, support disparate usage scenarios within and beyond the enterprise, and encourage widespread adoption, enterprises need a versatile, all-in-one authentication platform that supports a rich set of strong-authentication methods and devices. The authentication platform must be able to consolidate multiple forms of authentication onto a single device, and it must provide unified interfaces and management services that work across all forms of strong authentication. VeriSign calls this innovative, holistic approach unified authentication.

VeriSign Unified Authentication is based on OATH's vision of universal strong authentication and is intended to enable widespread adoption of strong authentication by reducing its cost and complexity.

Implementing a comprehensive, fully integrated strong-authentication solution is a complex task. Whether authentication is deployed in premise or outsourced to a reliable provider, it should meet the following requirements:

- **Integrated platform** – For maximum flexibility and consistent enforcement of security policies, the enterprise should be able to provision and manage all authentication credentials, users, and devices from a single, integrated management system that supports multiple credential devices.
- **Leveraged infrastructure** – To decrease costs and speed deployment, the authentication solution should leverage existing identity-management infrastructure such as user stores (directories and relational database management systems (RDBMS)), RADIUS, and single sign-on (SSO) servers.
- **Flexible security devices** – To increase user convenience and enable partners, suppliers, and mobile employees to access resources, the solution should be capable of consolidating credentials onto a single, portable device. This should be true whether the device is a key fob or a standard smart card. Preferably, the solution should minimize or eliminate the installation of new client software.
- **Built-in reliability** – To accommodate growth and ensure 24x7 availability, the authentication solution must have highly secure, Internet-scale capabilities.
- **Open standards** – To leverage existing infrastructure, create best-of-breed solutions, and facilitate integration across application and network infrastructure, the authentication solution should use open standards such as X.509, RADIUS, the Lightweight Directory Access Protocol (LDAP), and Open Database Connectivity (ODBC).
- **User self-service** – To reduce management and support costs, increase user convenience, and enhance scalability, the authentication solution should allow users to perform—at the enterprise's discretion—lifecycle-management tasks (such as token activation, password replacement, and certificate renewal).

+ VeriSign Unified Authentication Solution: Value, Flexibility, Longevity

The VeriSign Unified Authentication solution meets requirements for unified authentication by providing an open, integrated platform for managing all types of two-factor authentication credentials. As espoused by OATH, the VeriSign Unified Authentication solution is built on open industry standards and leverages existing enterprise infrastructure. It reduces the cost of deployment not only by minimizing infrastructure requirements but also by moving the complexity of security, scalability, and reliability to VeriSign. Multipurpose next-generation tokens and self-service management capabilities to further reduce TCO for a total savings of up to 40 percent. Strong-authentication credentials can be used on enterprise desktops (plugged mode) or independently of the desktop (unplugged mode) via the VeriSign tokens, which allow users to conveniently carry security credentials with them. Using the VeriSign Unified Authentication solution, enterprises gain the control, flexibility, and long-term agility needed to take rapid advantage of emerging opportunities for online collaboration and commerce—now and in the future.

Single Platform, Multiple Credentials

VeriSign Unified Authentication is the first unified strong-authentication solution. By supporting multiple independent authentication credentials (dynamic OTPs, token-generated digital certificates, and desktop digital certificates) on one integrated platform, it enables enterprises to leverage a single platform for all their strong-authentication needs. In addition, the VeriSign solution is built on known, open standards, allowing easy integration into an enterprise's existing environment and keeping the door open for future innovation and best-of-breed technology.

Multipurpose Next-Generation Tokens

Multipurpose next-generation tokens are a core component of the VeriSign Unified Authentication solution. These cost-effective tokens can be used in plugged mode or unplugged mode. They can generate OTPs as well as store device or user certificates, thereby allowing employees, partners, and customers to use authentication credentials from remote locations. Other multipurpose devices (such as smart access cards with OTP capabilities built in to the smart-card OS) are under development. In addition to multipurpose next-generation tokens, VeriSign Unified Authentication supports PKI-only USB tokens.

Deployment Flexibility and Scalability

For maximum flexibility and scalability, the VeriSign Unified Authentication solution allows enterprises to deploy solution components completely in premise or to leverage VeriSign's unique network-security infrastructure. For example, an enterprise can start deploying strong authentication as an in-premise solution and then migrate to a fully outsourced model as scaling requirements increase or as strong authentication is extended to business partners and other external users (federated strong credentials).

In the fully outsourced model, VeriSign handles the complexity of deploying, securing, managing, and maintaining the infrastructure for the second authentication factor. Using this model eliminates the up-front costs and ongoing expenses associated with in-house authentication software and infrastructure. It also solves the scalability, reliability, and third-party trust issues that are difficult and costly for individual enterprises to surmount. Control remains with the enterprise, which still manages all user identities, user applications, and customer interactions.

+ Solution Components and Architecture

As Figure 1 shows, the VeriSign Unified Authentication solution includes the following components:

1. Strong credentials (including a next-generation secure token)
2. Provisioning and lifecycle services
3. Management services
4. Validation services
5. Self-service applications
6. Application integration

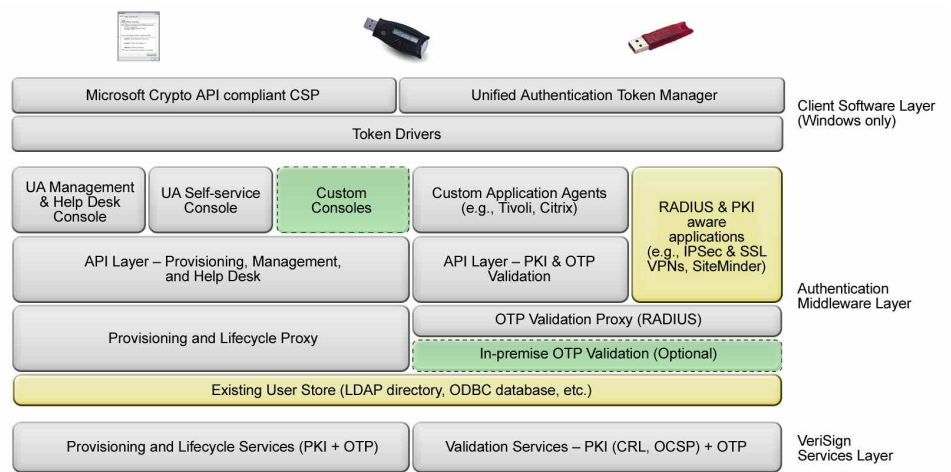


Figure 1: Unified Authentication-System Architecture

Strong Credentials

The VeriSign Unified Authentication solution supports multiple forms of two-factor authentication, as described in the following text.

First Factor

The first factor, “what you know,” is typically a static password or PIN. With this approach, users have only one password to remember, and the password can be managed centrally within the user store. The user store is typically an LDAP directory or a high-performance RDBMS such as Oracle®. For PKI tokens, the first factor is typically the PIN used to unlock the token or smart card.

Second Factor

The second factor, “what you have,” can be either an OTP or an X.509 certificate. Credentials can be either soft (that is, stored on the desktop) or hardened using cryptographic hardware such as a USB smart card, an OTP token, or a smart card.

- **Hard OTP** – The second factor is a dynamic, token-generated OTP. The token device has a display and a battery and can function without being connected to a computer. It does not require any client-software installation.

- **Soft OTP** – The second factor is a dynamic OTP generated by a small client application running on the user desktop.
- **Hard certificate** – The second factor is a user X.509 digital certificate capturing the user identity and stored in the secure hardware device. The certificate can be based on a certificate template, allowing multiple applications for the same certificate, such as smart-card logon, 802.1x authentication, Web-application authentication, and Secure Multipurpose Internet Mail Extensions (S/MIME).
- **Soft certificate** – Optionally, the second factor is a user X.509 digital certificate capturing the user identity but stored on the user desktop.



Figure 2: Secure Token Capable of OTP and PKI Authentication

Multipurpose Next-Generation Token

VeriSign's Multipurpose Next-Generation Token (see Figure 2 above) is one of the first all-in-one security tokens introduced to the market. This cost-effective token supports both OTP and PKI authentication and can also store smart card information.

OTP authentication is performed in “unplugged” mode; that is, the user does not have to plug in to a USB port, smart-card reader, or other device. OTP authentication is ideal for allowing partners, customers, and remote employees to access extranets and VPNs from kiosks, personal digital assistants (PDAs), and home offices. To obtain an OTP, the user presses a button on the token to trigger the next OTP value, and the resulting value is displayed on a small LCD. To access a resource, the user enters this value, along with his or her user ID and static password, into the application's password field.

For added functionality and more secure access to resources, enterprises can opt to use the token's built-in PKI support. “Plug and go” PKI support allows not only authentication but also encryption, and digital signatures for nonrepudiation. To enable digital certificate-based functions, the token must be plugged in to the client desktop via the token's USB connector. In addition, drivers must be installed on the client desktop to enable communication between the user desktop and the token cryptographic processor.

For all cryptographic operations, the token leverages a secure Infineon® smart card embedded into all tokens. The smart card contains up to 64K of onboard, electronically erasable programmable read-only memory (EEPROM), which is used primarily for storing digital certificates.

The cost of issuing a token to a user is fixed, regardless of how many functions it enables. To help enterprises extract maximum value from their investment, VeriSign is committed to continually broadening the range of security functions that a single device can perform. In the future, the capability to embed flash storage and radio-frequency identification (RFID) capabilities into the onboard chipset will transform VeriSign tokens into powerful, cost-effective platforms for deploying a broader range of security applications such as physical-building access, secure storage, and end-point protection.

Validation Services

Strong authentication requires validation of both authentication factors. First-factor validation typically occurs at the enterprise. Depending on the selected deployment model, either VeriSign or the enterprise can perform second-factor validation of an OTP.

First-Factor Validation

The first authentication factor is based on a user name and password (PIN). For OTP, this information is stored in the enterprise's user store (LDAP or RDBMS store); therefore, the first factor is validated locally. The process involves a fast local-directory or database lookup.

Second-Factor Validation

Depending on enterprise requirements, VeriSign can perform OTP validation as an in-the-cloud service or the enterprise can do so using an in-premise version of the VeriSign Unified Authentication solution.

To integrate the OTP validation service, VeriSign provides a small RADIUS proxy. This stateless server integrates with both the local directory (using the LDAP protocol) and the enterprise validation engine. RADIUS proxy-based deployment is ideal for network applications such as VPN remote access.

For PKI, the certificate is typically verified locally in the application, and revocation status is checked using either a certificate-revocation list (CRL) or the real-time Online Certificate Status Protocol (OCSP).

Alternatively, VeriSign provides a small validation software-developer kit (SDK) in C or Sun Microsystems® Java®. The SDK allows IT developers to directly integrate VeriSign two-factor authentication into existing applications and server infrastructure. For example, a Sun Microsystems® Java 2 Enterprise Edition® (J2EE) application that already performs one-factor authentication against a database can easily integrate second-factor validation into the existing access-control Java code base (as a new Java class or Sun Microsystems® JavaBeans® entity).

In-the-Cloud Validation Utility

To ensure maximum reliability, scalability, and security, VeriSign deploys OTP validation on top of its proven domain-name system (DNS) infrastructure, Advanced Transaction Lookup and Signaling™ (ATLAS). The exceptionally robust infrastructure resolves more than 14 billion DNS queries per day and consists of 14 globally distributed data centers. In addition, this infrastructure has maintained an effective uptime of 100 percent for the last seven years. The DNS constellation routinely withstands more than 1,000 attacks a day, and successfully turned back the largest denial-of-service attack in history—the only DNS root-zone servers supporting the Internet not to succumb to the attack.

In-Premise Validation Engine

Optionally, the VeriSign Unified Authentication solution can be deployed in premise to validate the second factor (OTP value). In this case, the in-premise OTP validation server validates the OTP using a high-performance database and optimized front-end validation engines.

Figure 3 shows OTP validation deployed within the enterprise. To support in-premise validation, the enterprise must deploy OTP validation engines. Validation engines are stateless, high-performance software that can be scaled linearly depending on enterprise requirements. Token information—including shared-secret and operational information like the current count value—is stored in the OTP store, as shown in the figure. VeriSign recommends that enterprises use an optimized database for the OTP store.

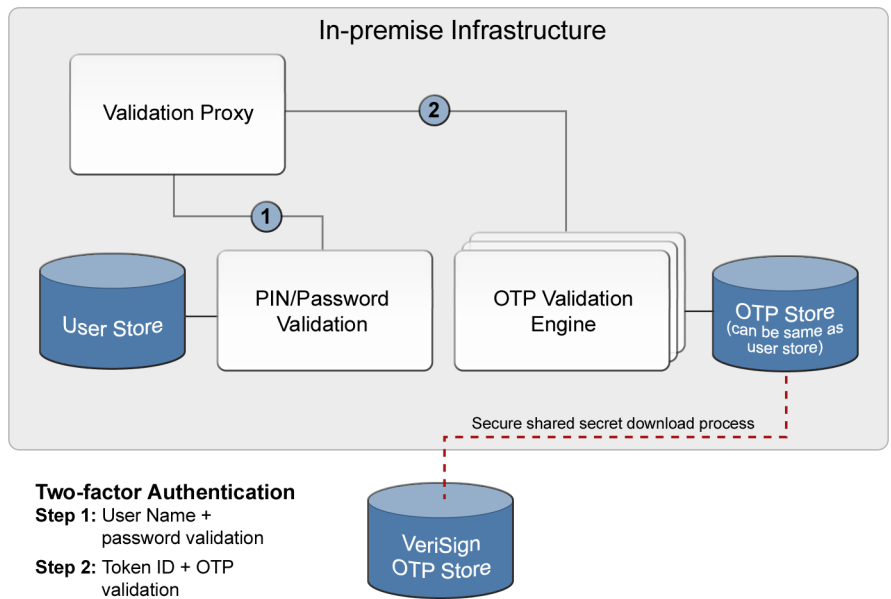


Figure 3: Deployment Scenario: In-premise OTP Validation

As part of the token manufacturing process, the token information is registered in the VeriSign OTP store. In the case of in-premise validation, this information would be transferred from the VeriSign OTP store to the enterprise OTP store using a secure batch process, as shown in the diagram.

Provisioning and Lifecycle Services

The VeriSign Unified Authentication solution includes three provisioning and lifecycle services: new-credentials issuance, token activation, and certificate renewal.

New Credentials Issuance

The credentials-issuance service supports all forms of two-factor authentication credentials (OTP secret and digital certificate). In the case of the OTP, the credentials-issuance service is not required, because OTP secrets are embedded at manufacturing time. However, the administrator or user must activate the OTP token.

In the case of user certificates, the VeriSign Unified Authentication solution can integrate with Microsoft Windows Server® 2003 and utilize the user automatic-enrollment capabilities in Microsoft Windows® XP to simplify certificate deployment and renewal. Automatic certificate enrollment provides a quick, simple way to issue certificates to users and to enable PKI applications; it reduces the complexity of PKI deployments and minimizes the total cost of ownership for a PKI implementation. The auto-enrollment process is triggered as part of the Windows reboot or logon operation and is transparent to end users. Certificates within the enterprise-defined “renew period” are also renewed transparently.

Token Activation

This operation activates the token for two-factor authentication using the OTP; it does so by making the necessary binding between the token and the user in the user store. VeriSign Unified Authentication supports two activation models: early-binding and late-binding activation. In the early-binding model, the system administrator activates the token on behalf of the user. The second model is a self-service approach in which any token can be sent to the user. Because it reduces administration and support costs, self-management is a key component of the VeriSign Unified Authentication solution.

Certificate Renewal

OTP credentials do not have to be renewed. User certificates, on the other hand, expire periodically (typically every year) and must be renewed. Using Windows Server 2003, the VeriSign Unified Authentication solution can utilize the auto-enrollment capabilities in Windows XP to automatically renew certificates as specified for each template. This capability significantly reduces the complexity of client certificate-lifecycle management.

Self-Service Applications

The built-in VeriSign Unified Authentication self-service applications help minimize support costs by enabling users to perform most lifecycle operations on their own. Users can access self-service applications via the following interfaces:

- Unified authentication Web interface: Enables users to access self-service applications via a Web interface to enterprise-hosted token-management services.
- Existing interface: To enable integration of the user self-services into existing user portals, provisioning systems (such as the IBM® Tivoli® Identity Manager™), or customer-support applications, VeriSign also provides an integration SDK.

As shown in Figure 4, besides enabling new-credentials issuance such as OTP token activation or certificate auto-enrollment, the self-service applications enable users to perform the following tasks:

- Change their PIN
- Reset a forgotten PIN
- Synchronize a token
- Replace a lost or broken token
- Enroll for new certificates or renew existing certificates



Figure 4: The VeriSign Unified Authentication self service portal

Management Services

The VeriSign Unified Authentication solution supports help desk and administration functions by providing tools for lifecycle-management tasks including issuance, revocation, tracking, and auditing of strong credentials.

Administration Services

Administration services provide authorized access to all self-service applications, all help-desk functions, and restricted operations such as token and certificate revocation. Administrators access these functions through a Web interface.

Other important administration functions include manual token assignment (early-binding activation) and manual token activation. Although the default token-distribution model assumes no prebinding until the user self-activates the token, these functions enable an administrator to manually bind a token to a specific user within the enterprise's user store and to activate the token, too.

Audit Trails

The VeriSign Unified Authentication solution records all significant events by transaction. The service creates audit trails for all OTP transactions, including passed and failed validations, activations, and PIN resets. It also creates audit trails for PKI transactions such as requesting, creating, and revoking certificates.

User-administration audit logs record functions executed by individual administrators, and changes administrators make to the registration-authority (RA) configuration are logged in a policy file. Also, audit records are maintained independently in multiple media depending upon the sensitivity of the event, and reconciliation of the audit trails is periodically verified. All audit logs are subject to retention policies that meet or exceed industry standards and are examined at least weekly for significant security and operational events. In addition, VeriSign reviews its audit logs for suspicious or unusual activity in response to alerts generated within VeriSign Unified Authentication systems. Should significant security-related events occur, VeriSign alerts the enterprise's designated information-security contact.

Application Integration

As discussed earlier, the VeriSign Unified Authentication solution provides a truly open architecture based on industry standards such as LDAP, RADIUS, X.509, and Public Key Cryptography Standards (PKCS). The VeriSign solution leverages these standards to interoperate automatically with a number of network and business applications that require authentication, such as Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL) VPNs that natively support both X.509 and RADIUS-based authentication. (See Figure 5 below.)

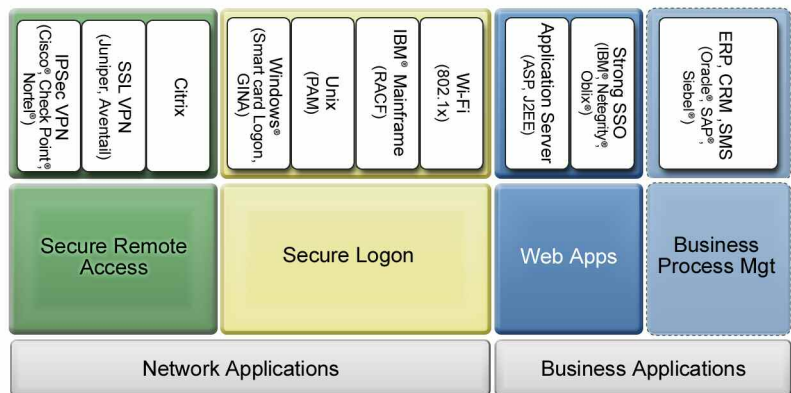


Figure 5: Unified Authentication: Application-Integration Support

For applications in this figure that do not natively support RADIUS or PKI, the Unified Authentication solution provides a set of custom agents. These agents are built on top of the solution's validation application programming interfaces (APIs).

Finally, VeriSign also provides a small validation software developer kit (SDK) in C or Java that allows IT developers to integrate VeriSign two-factor authentication into their custom application environment.

+ Solution Scenarios

This section describes some of the typical solution scenarios for VeriSign Unified Authentication.

Secure Remote Access

With an increasingly mobile workforce, secure remote access to employees is becoming an essential IT requirement. Remote access is typically provided using traditional IPSec VPN or the newer SSL VPN appliances.

Most VPN products (IPSec and SSL) natively support RADIUS-based authentication as well as certificate-based authentication. To configure a VPN box to accept PKI-based authentication, an enterprise typically needs to configure the root CA in the VPN management consoles. For OTP authentication, the enterprise can point to the Unified Authentication validation proxy, possibly specifying a backup proxy if more than one proxy instance is deployed within the enterprise.

Figure 6 shows the typical deployment for secure remote access using the VeriSign Unified Authentication solution. End users can use the solution's default self-service console. Support staff can use the solution's help desk console to manage the tokens for those users.

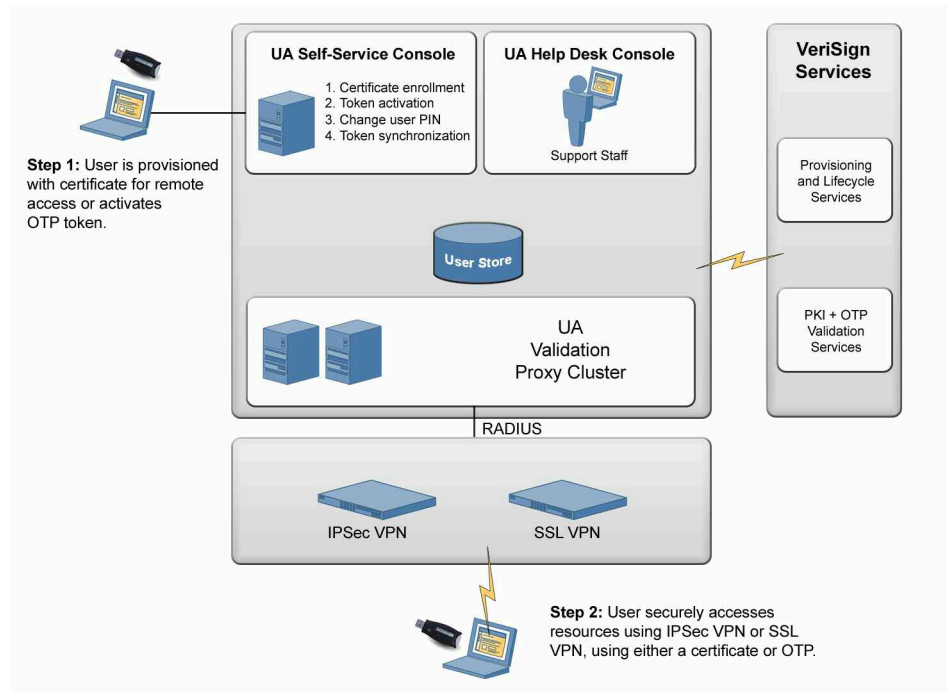


Figure 6: Application Scenario: Secure Remote Access

Banking Web Application

To provide additional security, financial institutions frequently want to enable premium customers to use two-factor authentication to access their online accounts. In the scenario illustrated here, the bank has an existing sign-up process for online banking and wants to provision tokens as part of the sign-up process. It also has a self-service portal for end users as well as a help-desk console for its customer-service representatives.

As seen in the Figure 7, the bank uses various VeriSign Unified Authentication APIs to integrate provisioning, self-service, and help-desk functionality for Unified Authentication tokens into its existing Web consoles/applications.

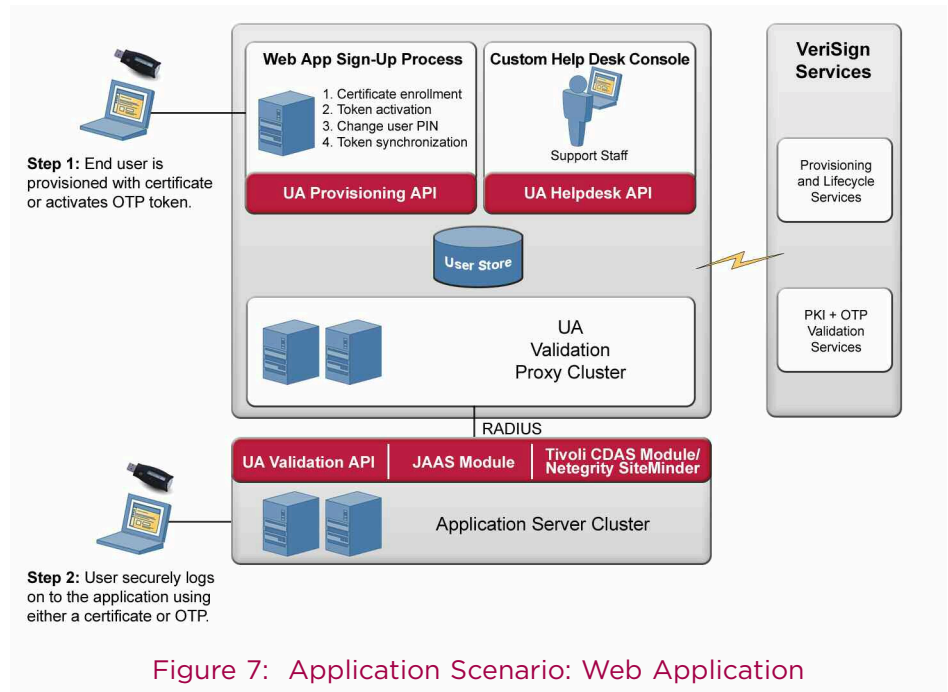


Figure 7: Application Scenario: Web Application

Depending on the Web application’s specific environment, the bank can use one of the following approaches for OTP validation:

- If the bank application is a J2EE application, the bank can use the Unified Authentication Sun Microsystems® Java Authentication and Authorization Service (JAAS) module for OTP validation. J2EE natively supports PKI validation.
- The VeriSign Unified Authentication solution integrates with leading access-management products either natively (such as Netegrity® SiteMinder® via the XAuthRADIUS authentication scheme) or via custom agents, such as the Unified Authentication solution’s Computer Directory Assistance System (CDAS) module for IBM’s Tivoli Access Manager). If the bank application uses one of these access-management products, it can leverage this integration to support two-factor authentication.
- If the bank has a custom Web-application environment, it can use the Unified Authentication validation APIs (both C and Java APIs are available) to integrate two-factor authentication into its application.

Token Co-existence

In some cases, enterprise users may already have one time password (OTP) tokens from another vendor. To protect its existing investment, an enterprise may want to phase in VeriSign Unified Authentication tokens as existing tokens expire.

Figure 8 shows the token-migration feature of the VeriSign Unified Authentication validation proxy. The scenario is similar to the secure-remote-access scenario described earlier. The administrator can configure an external authentication server called the delegation server. (Note that the external authentication server must support RADIUS.) Upon receiving a request, the validation proxy always checks to see whether the user has a valid VeriSign Unified Authentication token. If a token is enabled against the user name in the user store, the validation proxy will validate the supplied credentials as usual. However, if no VeriSign token is enabled, the validation proxy will attempt to authenticate the supplied credentials against the configured delegation server.

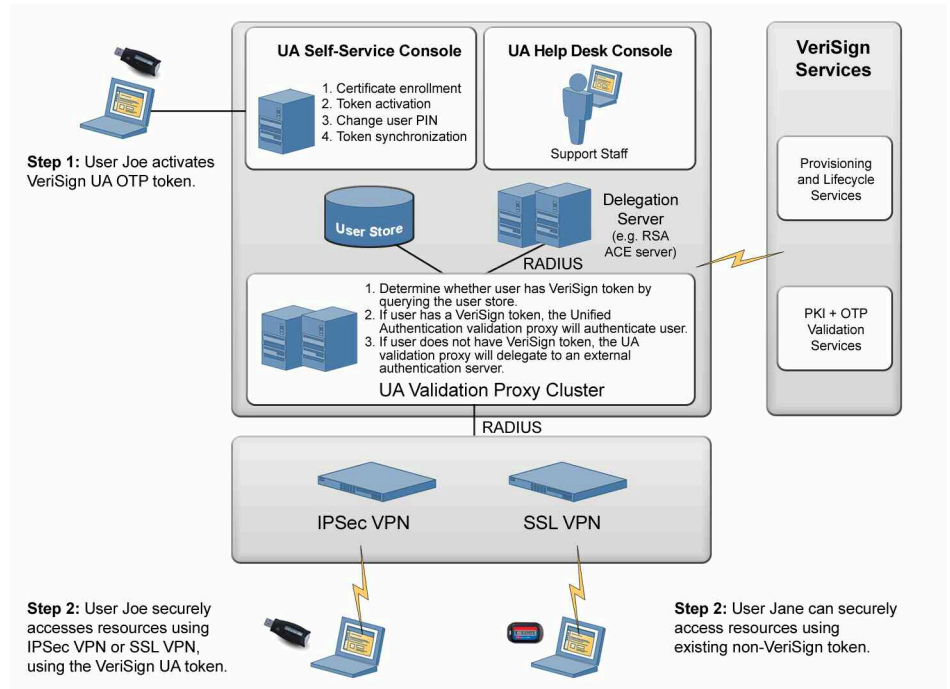


Figure 8: Application Scenario: Token Co-existence

In this scenario, Joe can securely access his enterprise resources using his PIN and the VeriSign Unified Authentication token, while Jane can use her SecurID® token to access resources.

+ Conclusion

Strong authentication is essential to cultivating a truly seamless, dynamic Internet, where all people and all devices can be reliably identified in an open, interoperable, and federated environment. Although existing proprietary strong-authentication software resolves problems related to network access, its complexity and high cost of ownership create barriers to adoption. Lack of interoperability and flexibility, limited integration, poor scalability, and infrastructure and hardware costs are the key contributors to this problem.

The VeriSign Unified Authentication solution addresses these issues by enabling enterprises to leverage a single integrated platform for all their strong-authentication needs. It reduces the cost of deployment by leveraging an enterprise's existing infrastructure and moving the complexity of security and scalability to VeriSign. Based on guidelines developed by OATH, the open-reference architecture provides a common interface for managing all types of credentials from multiple vendors. By reducing the cost and complexity of strong authentication, the Unified Authentication solution enables more ubiquitous adoption of strong authentication, thereby propelling enterprises to the next level of innovation, sophistication, and complexity in online collaboration and commerce.

VeriSign Unified Authentication Solution: Key Differentiators

Besides meeting key requirements for strong authentication, the VeriSign Unified Authentication solution distinguishes itself from competing solutions by delivering the following benefits:

More Value – VeriSign Unified Authentication provides a single integrated platform for all strong authentication needs:

- It allows multiple credentials on a single platform (OTP, USB token, certificates, and smart card).
- It supports all user types (employees, partners, and customers).
- It includes multipurpose next-generation tokens that can be used in unplugged mode for OTP validation or in plugged mode for digital certificate-based authentication.

Less Costs – VeriSign Unified Authentication delivers up to 25–40 percent lower TCO than other two-factor authentication solutions:

- It uses cost-effective multipurpose next-generation tokens.
- It allows re-use of existing infrastructure (directory, AAA servers, SSO middleware).
- It includes user self-service modules to decrease support costs.
- It reduces deployment and ongoing management and maintenance costs (when enterprise adopts the outsourced service model).

Designed To Fit – VeriSign Unified Authentication leverages existing technology investments and offers flexible deployment options:

- It uses common open standards such as X.509, RADIUS, LDAP, and ODBC to enable enterprises to leverage existing infrastructure.
- It enables enterprises to leverage their central user directory, user provisioning and SSO middleware, AAA (RADIUS) servers, and administration tools.
- It integrates and deploys easily (unlike some proprietary, software-based models).
- It allows enterprises to run validation at VeriSign or in premise.



Future Proof – VeriSign Unified Authentication provides a holistic, open solution that can accommodate technology advances, long-term growth, and evolving business requirements:

- It prevents enterprises from being locked in to proprietary solutions and allows best-of-breed solutions.
- It supports strong authentication using smart cards, device-generated OTPs, and digital certificates.
- It supports PKI-based encryption, digital signing, and nonrepudiation.

+ For More Information

For more information about the VeriSign Unified Authentication solution, please contact our Unified Authentication Specialists at 650-426-5310 or email enterprise_security@verisign.com.