VeriSign® The Value of Trust℠

Open Authentication

A Vision for Strongly Authenticating All Users, All Devices, and All Applications Across All Networks

CONTENTS

Although strong identity credentials are crucial to the continued growth and vitality of online business, the expense and complexity of strong authentication solutions frequently impede their adoption. To address this issue, a new vision for strong authentication has emerged. Based on the open authentication roadmap espoused by the Open Authentication (OATH) industry partnership, this vision calls for the creation of a common, open- standards-based authentication platform, where enterprises can authenticate all users, all devices and all networks, all the time. VeriSign has embraced this vision to help enterprises more freely cultivate new business opportunities, embrace advanced technologies, and move strategic processes online. Leveraging the dynamic strength of its infrastructure, technology, data and intelligence resources, VeriSign's coming generation of strong authentication services moves authentication to a "network services" architecture that promotes ubiquitous adoption of strong authentication by reducing complexity and lowering total cost of ownership.

Proprietary vs. Open Systems –The Rise of Open Networking

In the 1970s, large companies were reluctant to trust unreliable networking technology to automate critical transactions. In response, IBM developed a suite of protocols and products to connect mainframes to local terminals, printers, and computers. These solutions were based on proprietary protocols such as Systems Network Architecture (SNA) and token ring, and had unprecedented benefits. Instead of taking hours or days to move data using tape, the same task could now be done in seconds or minutes. Companies began to build networks and use them for mission-critical applications.

These early networks depended on expensive and dedicated switching computers managed by a centralised mainframe. They worked well as long as a specialised professional staff installed and managed all the communication equipment. The network design was astonishingly complex, and only IBM had all the necessary elements. Because of its centralised design, if the network failed, the entire company could be temporarily out of business. In a nutshell, the solution was expensive, complex and inflexible. Yet it solved important problems, and customers were satisfied with their deployments, as there were no alternatives.

In the 1980s, a new set of needs emerged. Minicomputers replaced mainframes, and personal computers replaced terminals. Distributed computing, using components from multiple vendors, became the norm. A radical shift towards open, interoperable and simple networking standards became imperative.

TCP/IP provided that open framework and transformed our world. The 1990s saw the massive, global deployment of networking technology in businesses and homes. IP networking enabled usage scenarios that early adopters of SNA and token ring technology could not even imagine.

The migration from proprietary to open standards is an inevitable step in the evolution of all technology. Existing proprietary authentication solutions address a small portion of the online security problem, but new threats and emerging opportunities demand a more mature approach. Authentication provides the necessary foundation for making the Internet a truly secure

medium for communication and commerce. As with networking, ubiquitous authentication will come only with the shift from proprietary to open architecture. This ubiquity will enable a future that today's adopter of proprietary solutions cannot fully envision.

Reaching for the Brass Ring

The commercialisation of the Internet has fundamentally transformed the way in which businesses operate. This revolution has opened up tremendous revenue opportunities and productivity improvements. Indeed, the market estimates that more than 48% of the productivity gains made over the next ten years will come through the application of Internet technology. Despite widespread perceptions that online business activity has slowed since the "bubble" burst in March 2000, the Internet has, in fact, continued to grow at impressive rates. Daily Web interactions have shot up by more than 500%, and e-commerce transactions have grown by an astounding 74% annually.

Yet increased usage brings increased risk. Online identity theft continues unabated, and stolen identities are being used for an increasing number of malicious activities ranging from spam to fraudulent credit card transactions, to orchestrated security attacks using compromised computers. Analysts estimate that more than $15 billion has gone unrealised due to trust issues in the commerce and communications arenas. Our inability to strongly authenticate users prevents the Internet from becoming a truly secure medium for commerce and collaboration.

In addition, security issues continue to impede adoption of new technology and the migration of critical transactions to the Internet. The cost and complexity of authentication have hindered adoption of new technology such as voice over IP (VoIP). They have also hobbled the movement of mission-critical financial data, supply-chain management services and transactions from private to public networks, thereby preventing industry from leveraging the inherent openness, interoperability and cost- efficiency of the Internet.

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 e-mail via office desktop, wireless laptop, pager, cell phone or cyber café. In this environment, implementation and consistent enforcement of an overall security policy become more complex and costly, often forcing enterprises to make undesirable trade-offs. In balancing costs, risks and opportunities, enterprises may have to consider exposing themselves to greater risk, foregoing full exploitation of their existing investments, missing out on business opportunities, or diverting precious funds from core business operations.

Are Passwords Good Enough?

A password is the easiest authentication method to implement and to use. But is it good enough? As with many risk management scenarios, it is sufficient for many applications. Yet a password can be easily shared, stolen, or guessed, making its misuse the leading cause of identity theft. For example, orchestrated attacks such as "phishing" can dupe users into voluntarily disclosing their passwords to somebody posing as a legitimate entity, who then uses the password for malicious purposes. Weaknesses and vulnerabilities can be found in all areas of password implementation, including input, transmission, verification, and storage.

Furthermore, passwords address the need to authenticate people only, yet there is an increasing requirement to strongly authenticate every device or network element, as well. Because users must be able to access information from everywhere, enterprises must allow guest computers to connect to their networks to access resources. This demand, the proliferation of wireless technology for PCs and handsets, and recent uses of IP networks — for everything from voice transmissions to Web services, to supply-chain management, to critical operations like oil drilling — require unprecedented network security. A rogue network element, whether intentionally or unintentionally compromised, can infect and debilitate a network with a worm or other virus in minutes. And although passwords may be "good enough" for authenticating users, they are not a viable alternative for machines and applications.

Clearly, a strongly authenticated public and private network is a necessary evolutionary step for securing the Internet, and will lay the foundation for the next wave of innovation.

What If?

What benefits are realised if strong authentication credentials can be deployed for under $10 per user? What is possible if every user and every device is strongly authenticated on the Internet? What is the future that current adopters cannot even envision?

At a minimum, we can expect to reap the following benefits:

- significantly reduce credit card fraud, and thereby lower costs for merchants, banks, card associations and, ultimately, consumers
- increase user privacy by providing a unique credential that verifies an individual's identity without revealing personal information such as name or Social Security number
- create new revenue streams by enabling value-added subscription services for Internet and mobile service providers
- provide safe virtual communities for children or other special-interest groups
- enable key offline "transactions" such as voting
- speed the migration of voice applications, financial transactions and other critical services to the existing IP infrastructure
- and, increased trust – in users, and merchants, which is fundamental to ubiquitous eCommerce

VoIP Not Ready to Stand Alone

Although it had been an early adopter of VoIP, a leading financial management company recently replaced its IP-only telephony installations with a combination of IP and traditional telephony equipment. The firm made the move after experiencing a sharp rise in attacks on its IP network. As one of the world's largest managers of financial assets, the company wanted to avoid the risk of losing both voice and data services if its IP-only telephony network were compromised. To resolve the issue, the investment bank invested in a dual IP/TDM solution, which allows it to move ahead with an IP telephony strategy, while ensuring high availability via the time-division multiplexing (TDM) voice backup.

Stronger Mechanisms for Identity Authentication
The following mechanisms provide a higher level of security than passwords, especially when used with one another.v

Digital Certificates
Based on public key encryption, digital certificates serve as unique, unforgeable online credentials that authenticate the identity of each device or device user and identify privileges for authorised access to private online information. In addition to being a superior mechanism for identity authentication, digital certificates enable digital signing and encryption to provide the privacy, data integrity and non-repudiation services that passwords and PINs do not support.

Tokens/Smart Cards
Tokens and smart cards carry an embedded microchip that stores security data and applications. They hold more information than magnetic stripe cards, and can be programmed for a variety of applications. Multiple applications can reside on a single token, and applications may be added, deleted or upgraded without reissuing the token. Requiring a PIN to access credentials on the token provides an added layer of protection if the token itself is lost or stolen. Tokens can also be used with biometrics such as palm, fingerprint or retinal scanning to strengthen security.

Digital Certificates with Tokens
Digital certificates combined with tokens offer greater security, convenience and portability for Internet-based communication and commerce than either a digital certificate or token alone. Placing the digital certificate on the token provides more protection against theft, fraud, or impersonation than if it were stored on the user's hard drive. Networks, systems and applications are much less likely to be compromised. In addition, by incorporating one or more identification certificates on the token, users can carry with them the appropriate credentials to access systems remotely, severing ties to a single workstation.

Digital Certificates with TPMs
Trusted platform modules (TPMs) are isolated chips that reside on the computer's motherboard and use digital signatures to verify that the operating system and other components of the software environment have not been compromised. When combined with a digital certificate, they provide the strongest authentication.

The Need for Ubiquitous Strong Authentication

Strong authentication provides the foundation for more secure networks, where all people and all devices can be reliably identified. It is an essential requirement of trusted networks, where transactions can be conducted without compromise. Several factors are driving the need for strong authentication: the rise in identity theft, the evolution of federated identity networks and, most importantly, the desire to leverage the IP network infrastructure for recent innovations.

Rise in Identity Theft

As mainstream consumer services such as banking, health care and insurance complete their migration to the network, enterprises must ensure that credit card accounts, e-mail addresses, National Citizen numbers and other personal information cannot be stolen. A strong digital ID implemented in the form of a specialised device or integrated within traditional digital assistants and mobile phones reduces the very large number of points at which a global public network may be attacked.

Evolution of Federated Networks

With the introduction of network-based systems for managing corporate content, supply-chain data and customer services, enterprises are increasingly challenged to provide access to a very large and dynamic group of end users that includes remote employees, business partners and customers. The complexity and cost of managing identities across internal and external systems, combined with the necessity to open up access to data, has created the need for federated networks where identification, credentials, and attributes may be shared among partners. When an identity is shared, its strength determines security across the entire access control chain, creating complex dependencies and liabilities across multiple business and legal parties. Strong authentication is crucial for securing access across federated networks and achieving compliance with federal regulations related to data sharing, such as in Healthcare, Banking, Insurance, and Government markets.

Leveraging IP Infrastructure for New Innovations

IP infrastructure is a common, global asset the likes of which the world has never seen. It is the result of organic investment from countless entities. Its openness is the source of its power but also of its limitations. IP networking is still in early adolescence in terms of its ultimate impact, and security is a significant barrier to leveraging this asset to its full potential.

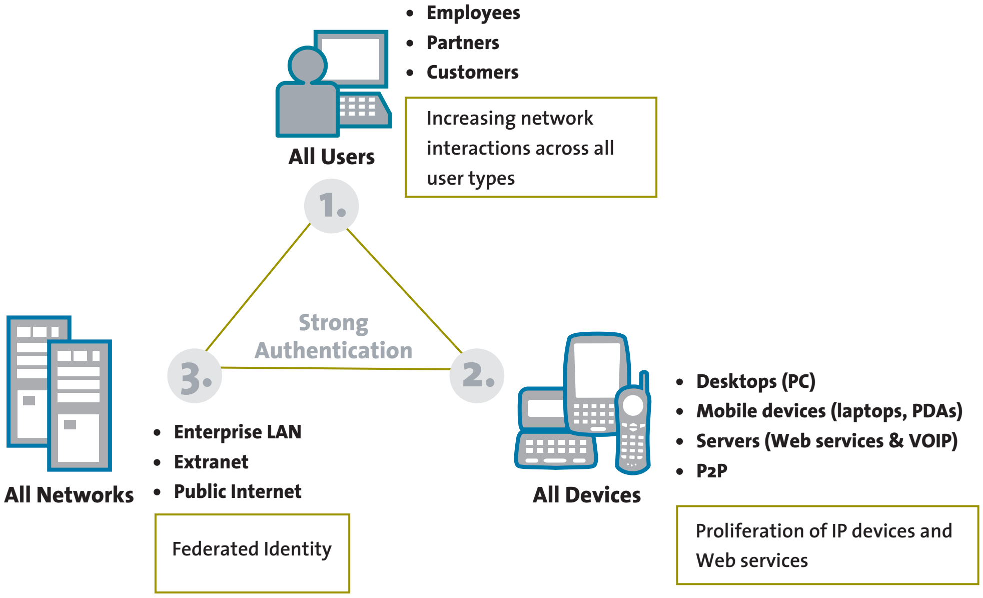
The capability to strongly authenticate people, devices and applications across all networks is an important prerequisite for propelling the use of IP network infrastructure beyond its current functionality. For example, leveraging IP networks for voice traffic can reduce costs significantly. However, achieving the level of reliability that exists in public switch telephone network (PSTN) technology requires IP networks to have an unprecedented level of security, which can be achieved only by strongly authenticating every network element. Similarly, the critical movement of money still occurs mostly over closed and private networks. Like voice over IP, leveraging the Internet for these transactions will lead to cost efficiencies, but will require high levels of authentication for people and applications.

Barriers to Ubiquitous Adoption of Strong Authentication Solutions

Although existing strong authentication solutions solve problems related to network access, their complexity and high cost of ownership create artificial barriers to wider adoption. Lack of interoperability, poor scalability, and initial and ongoing costs are the key contributors to this problem.

- **Lack of interoperability** – like early networking products, today's strong authentication solutions are proprietary and vertically integrated. They contain their own directory, provisioning and validation components, as well as authentication devices that work only with these components. Even within a single enterprise, IT departments are often forced to maintain multiple parallel instances for different applications or separate organisations.
- **Poor scalability** – although today's solutions are adequate for enterprise deployment, they do not scale to the Internet. They can support hundreds of thousands of users with millions of transactions per day, not millions of users with billions of transactions. They do not support the horizontal scaling or distributed points of presence that are necessary to achieve Internet scale cost-effectively.
- **High cost and complexity** – existing solutions consist of dedicated software and hardware components that require significant amounts of time and resources to implement and maintain. In addition, the authentication devices themselves (e.g. tokens, smart cards, and Universal Serial Bus (USB) tokens) are artificially expensive, and tied to proprietary provisioning and validation systems. These factors increase the cost and complexity of integrating authentication mechanisms into existing network and application infrastructure.

Open Authentication: Toward a New Vision for Strongly Authenticating Users, Devices, and Applications



To enable ubiquitous adoption of strong authentication across all users, all devices, and all networks, the technology must be easy to deploy, easy to use, affordable and interoperable. Just as with other evolutions of technology, moving to an open, modular architecture is a critical shift. By going from proprietary, enterprise-scale solutions to an open framework, authentication can become a standards-based network service that scales to the global Internet. Ultimately, by making strong authentication part of the network fabric, new types of secure interaction will become possible, and the entire user community will benefit.

Requirements for Open Authentication

For strong authentication to ripen into a critical enabler, adopters must implement the following measures:

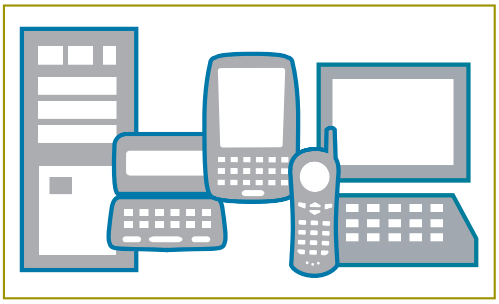
- **Standardize authentication devices** – use open standards to enable a flexible range of standalone and embedded credentials to be used across all applications.
- **Leverage existing middleware** – build on existing application and network infrastructure components without requiring additional hardware or software; leverage well-established protocols.
- **Federate and integrate identities** – leverage federated identity standards as a powerful mechanism for integrating authentication into internal and external applications.

Industry-Wide Collaboration

Authentication technology must migrate from proprietary, tightly coupled solutions to a radically new approach that embraces open standards and existing, best-of-breed infrastructure components. Migration toward open standards is essential to increase deployment. By laying the groundwork for ubiquity, integration and interoperability, an open architecture can decrease the risk and complexity of deploying strong authentication solutions, thereby driving adoption across enterprises, service providers and governments around the world.

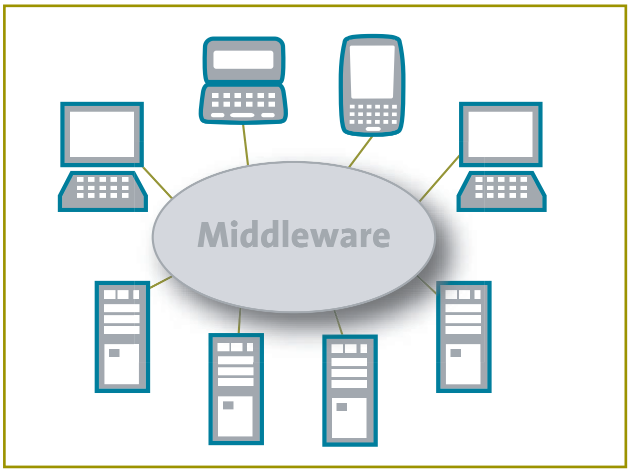
OATH - an industry group initiated by VeriSign - has created an initial roadmap for the collaborative development of an open strong authentication specification that can be adopted across the industry. This roadmap, which emphasises the use of existing technology and standards, is intended to provide 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.

Standardized Credentials...



Most authentication devices, from USB tokens to smart cards, are based on proprietary technology. One type of token cannot be used with another vendor's software. To simplify credential use and provide flexibility in the type of device or credential used, solutions should allow users to store, and manage on a common platform, all credentials based on One Time Password (OTP), PKI and subscriber identity module (SIM), using any type of device. OATH is bringing together the relevant companies to produce specifications for standardising the provisioning process and OTP algorithms. The specifications will be submitted to and standardised in organisations such as the Internet Engineering Task Force (IETF) and Smart Card Alliance. Ultimately, these specifications will proliferate in both standalone credentials such as tokens, and embedded credentials such as cell phones, PDAs, and laptops.

...Leveraging Existing Middleware



Another aspect of authentication integration is the leveraging of the existing network and application infrastructure to provision, manage, and validate strong authentication devices. Doing so eliminates the need for expensive parallel hardware and software infrastructure, as well as costly and complex integration.

OATH

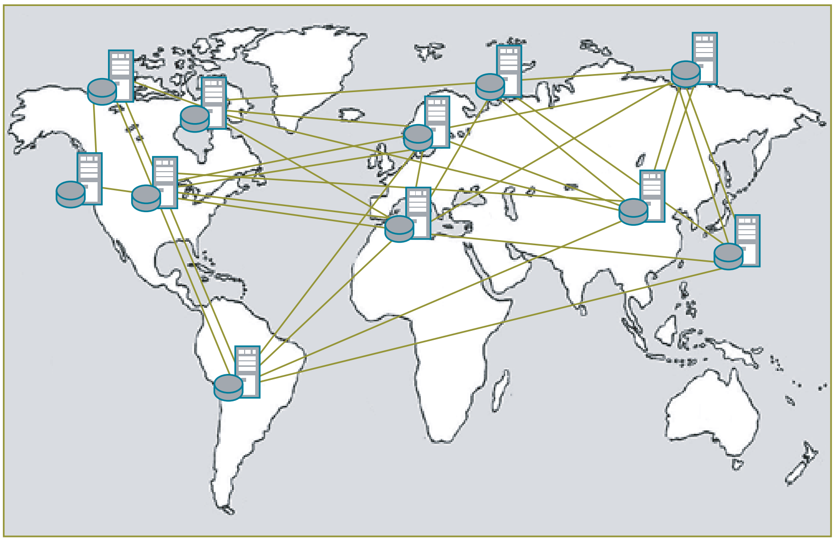
The Initiative for Open Authentication (OATH), an industry group initiated by VeriSign, is a collaboration among hardware credential providers (ActivCard, Aladdin Knowledge Systems, ARM, Axalto, Gemplus and Rainbow Technologies) to create a common platform based on open standards for managing both standalone (e.g. smart cards and tokens) and embedded (e.g. cell phones, PDAs and laptops) hardware credentials. OATH has been endorsed by leading network and application providers, including BEA™ and IBM®.

OATH relies on well-established protocols such as LDAP and RADIUS to allow existing networks and applications to provision and validate any OATH-compliant credential. This approach enables enterprises to deploy strong authentication without dedicated software and hardware, complex integration efforts or non-standard provisioning processes. For example, an enterprise using Microsoft servers and desktops can rely on standard Microsoft provisioning and directory services to provide strong credentials seamlessly to all its users. The same deployment is also possible for J2EE™ or other environments.

…Used Everywhere

Implementation of the OATH vision will enable the wide propagation of strong authentication credentials and other authentication components across many network end points (e.g. desktop computers, Web services servers, Wi-Fi access points and set-top boxes). OATH leverages existing federated identity standards to allow applications to validate credentials issued by other entities. This ability to trust and leverage credentials issued by third parties is a key enabler of interoperable transactions.

A New Internet Infrastructure Service



As strong authentication solutions are deployed en masse, the transactional capabilities (and costs) required to support identity validation and verification will move beyond individual enterprises to Internet scale. In effect, strong authentication will evolve from an enterprise service to a network service. The need for scalability will be compounded over time, as authentication systems track both current certificates and those that are no longer valid. This maturation requires a global infrastructure with the highest levels of performance and availability.

VeriSign: Paving the Way for Ubiquitous Strong Authentication

In coming months VeriSign, in conjunction with key partners, will introduce a strong authentication service. This service leverages the core specifications described in this white paper to move authentication to a "network services" architecture that fosters ubiquitous adoption of strong authentication by reducing complexity and total cost of ownership. Based on the guidelines developed by OATH, the open reference architecture will provide a common interface for managing all types of credentials from multiple vendors. The new service solution addresses VeriSign's long-term vision of ubiquitous strong authentication by accomplishing the following goals:

- an open, modular solution that leverages existing infrastructure and is easy to deploy
- a highly scalable network authentication utility to simplify authentication and enable identity federation
- lowers total cost of ownership

The initial version of the VeriSign Open Strong Authentication Service will focus on seamless integration with Microsoft servers and desktop applications to manage a variety of hardware credentials including OTPs, smart cards, PKI-based digital certificates, and hybrids. The solution is expected to be available Summer 2004. J2EE versions, offered in conjunction with other partners, are anticipated to follow shortly.

About VeriSign

VeriSign Inc. (NASDAQ:VRSN) delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate and transact with confidence.