



WHITE PAPER

---

# VeriSign® Identity Protection





**CONTENTS**

+ Introduction	3
+ Enabling the Digital Commerce Migration	5
Strong Authentication	5
Fraud Detection	6
+ VeriSign Identity Protection Services	7
VeriSign Identity Protection Authentication Service	7
VeriSign Identity Protection Fraud Detection Service	9
+ The VeriSign Identity Protection Network	10
VeriSign Identity Protection Shared Authentication Network	10
VeriSign Identity Protection Fraud Intelligence Network	11
+ VeriSign: A Trusted Partner	12
+ Related Research and Development	13
Mutual Authentication Services	13
Consumer Identity Management	13
Identity-Proofing Services	13
+ Learn More	14
+ About VeriSign	14



## VeriSign® Identity Protection

*“It is always very important for us to remember that our core business is to serve our clients’ needs. This means that every technology we choose has to perform appropriately without adversely impacting our clients’ experience on Schwab.com... The VeriSign team came across as a group of people that we could work with closely, and with whom we could have a long-term, productive relationship.”*

— Kostas Konstantinides  
Director of Client Web Services  
Charles Schwab & Co.

### + Introduction

More than ever, consumers are shopping or banking online for convenience and choice. This “digital migration” has led to the evolution of business strategies for diverse industries, including retail, financial services, media and entertainment, health care, and government services. For businesses, the opportunity is the development of a new distribution channel with the promise of increased sales and lower operating costs. Businesses are challenged, however, by the need to deliver a differentiated online customer experience while combating fraud and its negative effects.

Weak consumer authentication has fuelled the problems of Internet identity theft, phishing, and online financial fraud. As more consumers use computers and mobile devices for shopping, managing their finances, and accessing health care information, the risk of fraud and identity theft increases.

The root cause of much online fraud, identity theft continues to be a significant problem for enterprises and their customers. A recent Gartner survey reports that for the 12 months ending August 2006, more than 15 million Americans were victimized by some sort of fraud related to identity theft—a 50% increase from 2003, when the Federal Trade Commission reported 9.9 million victims. These incidents resulted in significant financial loss. According to Javelin Strategy and Research, total one-year fraud losses amounted to \$49.3 billion in 2007. Gartner estimates that the average loss in 2006 was \$3,257—more than double the average loss of \$1,408 in 2005.

While the losses themselves are significant, the problem is compounded by the negative impact on consumers’ confidence and, therefore, their buying behaviour. In the financial services industry, this can mean higher account churn, lower transaction volume, or a reduction in account assets. For other e-commerce applications, such as retail, gaming, or music and entertainment, this can mean lost revenue opportunities. A survey of U.S. households by Forrester Research showed that 24% of consumers did not make online purchases due to security concerns. A further 37% scaled back their online purchases for the same reason. According to a recent Gartner study, online-security concerns of 46% of U.S. adults led to over \$2 billion in lost sales in 2006. This data indicates that businesses have an opportunity to differentiate themselves and stand to gain significant revenue by addressing the security and trust concerns of the online consumer.

Once, only regulatory guidance around strengthened consumer authentication drove investment in technology. For example, the U.S. Federal Financial Institutions Examination Council (FFIEC), the Hong Kong Monetary Authority, and the China Banking Regulatory Commission all have regulatory initiatives related to online banking. Now, however, more and more enterprises are evaluating authentication options for their online consumer base as a means for business enablement.

Strong authentication has long been accepted in the enterprise as a technology to secure access to corporate networks and applications. However, the traditional deployment model presents significant cost and scalability problems when applied to the consumer market. Instead of thousands or tens of thousands of employees, the user population could be millions of consumers. In order to address the unique requirements of this segment, an entirely new approach to authentication is required.



VeriSign® Identity Protection (VIP) is a comprehensive suite of identity protection and authentication services that enable consumer-facing applications to provide a secure online experience for end users at a reasonable cost. VIP enables both a passive means of security through VeriSign Identity Protection (VIP) Fraud Detection Services as well as more active security through VeriSign Identity Protection (VIP) Authentication Services.

To minimise costs and maximise security by sharing intelligence and resources, VIP Services are enhanced by the effects of the VeriSign Identity Protection (VIP) Network. Inspired by the offline world of ATM networks, the VIP Network has two important distinguishing values: the sharing of authentication credentials and the sharing of fraud intelligence.

Credential sharing is enabled by the VeriSign Identity Protection (VIP) Shared Authentication Network where credential issuers and relying parties become part of a mutually beneficial trust network that enables consumers to use a second-factor credential on multiple Web sites. This provides convenience and greater security for consumers while allowing companies to share the cost of strong authentication infrastructure.

Because online fraud is often perpetrated as an attack on multiple online properties, the VeriSign Identity Protection (VIP) Fraud Intelligence Network further enhances the VIP Network by sharing intelligence among member companies. This “neighbourhood watch” approach allows companies to react quickly to mitigate the impact of online fraud.

VIP Shared Authentication possesses some unique qualities to help enterprises enable greater online revenue growth by protecting their consumers:

- **Convenient and Simple.** Users have a single, portable credential (such as a key fob token, credit card, or mobile phone enabled for a one-time password [OTP]) that serves as a second authenticating factor for any VIP network site—similar to those used in ATM networks.
- **Cost Efficient.** VIP is based on a shared service model in which VeriSign hosts infrastructure and Web services integration to minimise deployment and shared maintenance costs. A consistent user experience also minimises support costs for member sites.
- **Leveraged.** The sharing of authentication credentials can be leveraged to strengthen online affiliations and build channels. For example, an online retailer may be able to notify the eBay / PayPal community that their OTP token now works on its site (versus sites of competing retailers).
- **Standards Based.** In compliance with the open standards of the Open AuTHentication (OATH) reference architecture, no “vendor” lock is used for authentication credentials. VIP will work with any OATH-compliant form factor. Today, more than 70 manufacturers produce OATH-compliant solutions.
- **Trusted.** VeriSign has long been a provider of authentication services for over 900,000 Web servers—over 93% of the Fortune 500, the world’s 40 largest banks, and 43 out of the top 50 e-commerce sites. As a result, the VeriSign Secured™ Seal has high-level significance with consumers and has historically been associated with trusted commerce.

**SAMPLE REACTIONS OF CONSUMERS TO THE ROLLOUT OF OTP TOKENS BY A LARGE ONLINE AUCTION AND PAYMENT-PROCESSING SERVICE:**

*"Incredibly easy."*

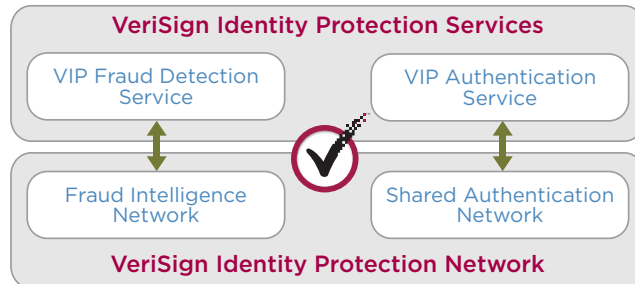
*"I love it—I'm going to make my password less complex because I'll always carry my security key."*

*"It is going to go with me everywhere."*

*"I think with the added security I'll take advantage of the 5.03% interest rate on cash deposited."*

*"A nice product I wish my own financial institution would institute."*

This paper explores how the core components of VIP work and how they fit together in the VIP Network.



**+ Enabling the Digital Commerce Migration**

Online shopping has enjoyed tremendous growth in the last decade, with the primary drivers being convenience and product availability. For the 2006 Holiday shopping season, over 66% of the U.S. online population shopped online. Marketers are perfecting the online user experience to offer customised purchase suggestions and further drive revenues for the online channel.

But a number of frictional forces prevent maximisation of online channels—and security is at the forefront. In a survey of over 5,000 online adults in the United States, nearly half say that concerns about the theft of information, data breaches, or Internet-based attacks have affected their purchasing payment, online transaction, or email behaviour. If this perception applies to half of all online U.S. adults, or more than 155 million people, it represents nearly \$2 billion in lost revenues.

Gartner recommends that enterprises take a two-prong approach to recover this lost revenue: Take measures to reduce fraud while at the same time increasing consumer confidence—in essence, marketing security measures as a business enabler.

VeriSign believes that the best way to prevent identity theft and fraud is through a layered approach: To help stop criminals from stealing identities, VeriSign recommends adopting strong authentication. To help stop criminals from successfully using stolen identities, VeriSign recommends adopting fraud detection.

**Strong Authentication**

The first line of defence against identity theft is strong authentication. Authentication is the process of validating the identity of end users. The goal is to distinguish between real users and imposters. The simplest and most common method for authentication with computers employs a user name and a single factor: a secret password. When users log in, the user names identify their accounts. The passwords prove that users are who they claim to be.

**Problems with Passwords**

In theory, this system works perfectly. Ideally, all end users choose passwords that are difficult for others to guess, choose a different password for each account, and never share these passwords with anyone else. Unfortunately, end users rarely choose good passwords, use different passwords for different accounts, or keep their passwords secret.

People usually choose simple passwords that are easy to remember, often using names, common words, and dates. Attackers know this and can often guess a password by using things they know about a person (such as a birth date, children's names, or other information) or by simply guessing random words and dates.



Most users have many accounts with different services. Few users are able to remember a different password for each account, and so choose a single password that they use on all Web sites. If the password for any site is compromised, then the password for all sites is compromised. Attackers can take advantage of this by creating a “free” Web site and requiring that users register for the service. Most users will select the same account name and password that they use for their email, bank, and e-commerce sites.

Finally, phishing email and Web sites have been used to defraud users. Many users have a difficult time distinguishing between real and fake Web sites and can be tricked into giving account information to a malicious third party.

#### **Adding Another Factor**

Multifactor authentication is designed to address these problems. A good authentication system will at least combine a primary factor (something the user knows) with a secondary factor (something that the user has or is). An attacker who steals only the first factor will not be able to forge the second factor and will be unable to authenticate. Similarly, an attacker who steals the second factor will not know the first and will be unable to authenticate. The many different types of secondary factors include hardware tokens, digital certificates, and biometric devices. Depending on an enterprise’s specific needs, an authentication system may require more than two factors. For example, a system might require a pass phrase, digital certificate, and thumbprint sensor, thereby combining something the user knows, something the user has, and something the user is.

#### **The Value of Consumer Trust**

In addition to taking steps to combat fraud, Gartner advocates building consumer trust as part of a strategy to gain or recapture revenue lost due to security concerns. The high-value / high-net-worth customer represents a segment that all online businesses covet; however, it is also especially targeted by online fraud. Understandably, this customer segment puts a high premium on security and privacy when doing business online. Regularly used strong authentication credentials can associate security as a brand attribute of online merchants or service providers. This, in turn, can benefit businesses by influencing customer loyalty.

#### *Fraud Detection*

Based on experience in traditional network security—and even military history—experts all agree that a “layered” security approach is best. Fraud detection provides effective protection against identity theft, and is a second line of defense when used in conjunction with strong authentication.

Many online users welcome additional security measures, but such protection sometimes requires additional steps during login and commerce transactions. As a first stage to deploying a comprehensive layered approach, many companies prefer the deployment of a passive means of fraud detection where the majority of consumers using the online channel are unimpacted when conducting commerce online. Authentication becomes risk based where only those behaviours outside of a normal user pattern are prompted for additional authentication. These powerful technologies can provide an intelligent and unobtrusive layer to combat online fraud.



### Detecting Suspicious Transactions

As creatures of habit, our actions often fit a pattern. For example, a user may log into his bank account and pay bills from his office in the city during the workday and log in from home in the suburbs over the weekend. What if a login transaction into the account is transmitted from a computer in Russia at dawn on a Thursday, and the transaction is a fund transfer of all the assets to a Swiss bank? This transaction is an anomaly—it does not fit the normal pattern for that user. Using sophisticated algorithms, fraud detection systems can “learn” normal usage patterns over time and detect if transactions do not match the patterns. This anomaly detection can be used to spot potentially fraudulent transactions.

Additionally, most companies have learned from experience that some transactions are inherently risky. Even if the machine learning system does not classify them as anomalous, some transactions are so suspicious that a company will want to double-check them. For example, an e-commerce site in Australia might want to double-check all international logins or all purchases greater than \$10,000. A complete fraud detection solution should allow companies to code rules like this to flag suspicious transactions.

### Identity Confirmation

Not every suspicious transaction is fraudulent. Because an end user may sometimes do something unexpected, some seemingly anomalous transactions may actually be legitimate. Rather than denying the transaction outright, a Web site fraud detection system should be complemented by an identity confirmation system. Such a system is automated to confirm an end user’s identity. These systems should support many different automated methods of confirmation without the involvement of customer support, including requesting a “secret question” response; having the user enter a PIN sent to them via email or an SMS text message or read to them in an automated phone call; or the use of a token-generated numeric code. This helps minimise the cost of identity confirmation to the Web site and minimises the inconvenience to the end user.

### + VeriSign® IdentityProtection Services

VeriSign® Identity Protection Services are a suite of layered services that enable enterprises to deliver trusted and safe online commerce to their customers, thereby increasing topline revenue and customer loyalty. VIP provides both visible and invisible mechanisms for securing online transactions and preventing identity theft. VIP Fraud Detection Service provides invisible server-side monitoring capabilities and VIP Authentication Service provides a more visible, standards-based strong authentication solution to ensure the identity of the consumer and protect the integrity of transactions.

#### *VeriSign® Identity Protection Authentication Service*

VeriSign Identity Protection Authentication Service provides strong, visible security for online commerce applications. The VIP Authentication Service allows a business to easily issue and/or accept multiple credentials from each user. It also provides comprehensive and highly flexible security available for consumer transactions.

VIP Authentication Service embraces open standards and allows any OATH-compliant device to be used for authentication. The solution offers serverless deployment and supports a wide range of credentials, including OTP tokens as well as “soft” devices such as voice-enabled OTPs, OTP-enabled mobile phones, and SMS OTPs.

**Credential Lifecycle Management**

For VIP customers who do not want to bear the burdens of credential issuance (such as token fulfillment, distribution, and support), VeriSign offers an outsourced solution—the VIP Portal—that issues credentials directly to end consumers. The service also provides first-level customer support directly to consumers. This allows enterprises to outsource the complexity to VeriSign, while also enabling strong multifactor authentication for their online application in a lightweight, easy-to-integrate fashion.

**Credential Validation**

VIP embraces open standards and allows any initiative for an OATH-compliant device to be used for authentication. OATH is an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication. By supporting open standards, the VIP Authentication Service solution can support a broad array of OTP form factors, from traditional hardware tokens to consumer-friendly devices, such as PDAs, USB flash drives, mobile phones, and dual-purpose credit cards.



VIP Authentication Service includes a number of options for supplemental factors, including stand-alone devices, such as OTP tokens, smart cards, and USB tokens, and “soft” devices, such as certificates, voice-enabled OTPs, and software for mobile phones. VIP makes it easy to offer any or all of these options to your customers today and to be prepared for tomorrow’s authentication choices. Web site developers can access VIP Authentication Service through a single set of APIs, regardless of the supplemental factors held by the end user.

**Integration with VIP Authentication Service**

VIP Authentication Service is implemented as an Internet service. Integration with Internet applications is straightforward, using a service-based interface. The result is seamless—users are unaware that sophisticated technology is behind the secure login.

**The VeriSign Identity Protection Portal**

For VIP customers who do not want to issue credentials to consumers directly, VeriSign offers the VeriSign Identity Protection Portal. This is a Web site that provides service and customer support to end users, including synchronisation for OTP tokens, repair or replacement of malfunctioning devices, and reporting lost or stolen devices.

*VeriSign® Identity Protection Fraud Detection Service*

The part of VIP that is invisible to the consumer is the VeriSign Identity Protection Fraud Detection Service. VIP Fraud Detection Service works in real time to detect and prevent identity theft and transaction fraud. It includes both a rule-based system and a unique behavioural heuristics engine. The service is designed to be simple and unobtrusive for both Web sites and end users. If the system detects suspicious transactions, end users can quickly provide additional verification to confirm their identities using an automated system. For example, the VIP Fraud Detection Service automated system may query the user to identify herself further with any of the following types of credentials: an OTP, a unique question and answer, a PIN provided to the user in email or SMS, or by phone or a customer service call.

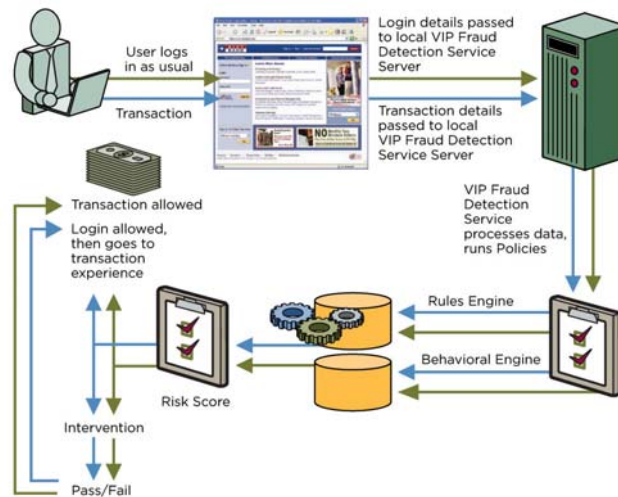
VIP Fraud Detection Service offers benefits because it is:

- **Invisible to the consumer.** VIP Fraud Detection Service does not change the user experience: Users log into the Web site in the same way that they always have.
- **Easy to deploy.** Because VIP Fraud Detection Service is a solution for the server side only, it requires no changes for the end user and minimal changes to the application.
- **Intelligent.** VIP Fraud Detection Service includes both rule-based systems and a self-learning behavioural engine to identify fraud.
- **Compliant.** VIP Fraud Detection Service is an economical way to address compliance with government regulations, such as the FFIEC rules in the United States and similar regulations outside the United States.

**Fraud Detection: How It Works**

The VIP Fraud Detection Service uses a combination of business rules and machine learning algorithms. The participating Web application passes information about transactions to VIP Fraud Detection Service, including the Web browser headers, IP address, and any other data. The VIP Fraud Detection Service system can then derive further information from the data before processing, such as determining the geographic location, connection type, and network provider from the IP address. Figure 1 below depicts the logical flow of user logins or transactions monitored by VIP FDS.

**Figure 1: VIP Fraud Detection Service Logical Flow for Login and Transaction Monitoring**





The first component of VIP FDS is an efficient rules-based system. Many companies have been fighting online fraud for years and understand the tactics used by criminals to steal money, goods, or identities. Additionally, VeriSign experts have identified many common patterns of fraudulent transactions. The VIP FDS rules engine allows companies to combine their own experience with the information provided by VeriSign. Participants can select from a set of predefined rules developed by VeriSign and can create their own rules using an intuitive user interface. Additionally, VeriSign professional services can help a business identify suspicious patterns and implement automated rules to find suspicious patterns unique to their environment.

The second component of the VIP FDS system is an automatic self-learning system for anomaly detection. Using state-of-the-art clustering algorithms, VIP FDS uses characteristics of user logins—Web browser type, IP address, time and date, account owner information, customer-defined cookies if present, and any other characteristics—to build a profile of normal user behavior. When a login attempt or other transaction does not match the previous pattern, perhaps because the login is from a different computer, on a different day, or in a different country, the VIP FDS system may flag the transaction as suspicious.

Once a transaction is flagged as suspicious, customers can invoke the VIP FDS system to pass the transaction to an identity confirmation system before authenticating the user. This second system asks the user for additional confirmation of identity, depending upon the degree of risk. The system may ask the user additional questions to confirm his identity or send a message using an out-of-band mechanism, such as a telephone call, SMS message, or email. If the user successfully confirms his identity, he will be logged in as usual. If the user cannot confirm his identity, the application can block the transaction or direct the customer to call customer service.

### **+ The VeriSign® IdentityProtection Network**

VIP Fraud Detection Service and VIP Authentication Service offer a compelling value proposition: a comprehensive, easy-to-deploy, and economical suite of services for reducing fraud, improving security, and achieving compliance. However, VIP offers much more than that.

The VIP Network is a set of shared services that builds on the VIP Fraud Detection Service and VIP Authentication Service. The VIP Network consists of two components: the VIP Shared Authentication Network and the VIP Fraud Intelligence Network. Each of the VIP services is enhanced by network effects: The first service helps businesses share authentication resources to reduce costs and improve the experience for end users. The second service helps businesses share intelligence about online identity fraud to improve security.

Customers may choose to subscribe to either service alone or to maximise the benefits of network membership by using both services. The VIP Network combines the two core VIP services in a unique business framework that facilitates sharing costs, data, and resources.

#### *VeriSign Identity Protection Shared Authentication Network*

Multifactor authentication can be costly for companies to deploy and maintain. A company must issue tokens to end users and provide training in the use of them, change applications to use tokens for authentication, assist users with lost or broken tokens and answer customer support questions about them, and dozens of other tasks.



Moreover, customers may resist multifactor authentication because it is unfamiliar and time-consuming. The VIP Network offers the benefit of shared authentication to address these issues. Much of the success of credit and ATM cards comes from their ubiquity: They can be used almost everywhere in the same way. Customers rarely encounter ATM machines where their cards do not work. We believe that end users will be more likely to adopt second factors if they can use the same device for all services and if the device works the same way for all services.

By sharing the authentication infrastructure between network members, the costs of adding and maintaining second factors is drastically reduced. By adopting the VIP standard, companies can ensure a simple and consistent user experience across the Internet. By outsourcing token lifecycle management to VeriSign, the burden of managing second-factor tokens and infrastructure disappears.

To facilitate this capability, the VIP Network is based on a framework for sharing resources and intelligence between network members.

#### **Roles in the Network**

The two roles in the VIP Network are issuer and relying party. A company that issues VIP Shared Authentication Network credentials to its customers is an issuer. A company that allows its users to authenticate using VIP Shared Authentication Network credentials is called a relying party. A company may play both roles—issue credentials to some users and accept from others the credentials issued by a third party. An issuer may include its own branding on tokens that it issues, but should also include the VIP Network logo. An issuer is the first point of contact for a customer on the VIP Network.

The credential issuer is also the point of contact for the end user. End users contact the issuer for first-level customer support questions, such as synchronisation problems and PIN resets. VeriSign can help with more difficult support issues and, optionally, with all customer support services.

An enterprise that is committed to strong authentication can issue its own tokens that are usable on the VIP Network. Issuers get all of the benefits of relying parties, along with opportunities to promote their brand through the token and better control of their end customers' Web experiences. The VIP Network is an easy way to secure users' Web lifestyles.

#### **Sharing Credentials**

To promote compatibility and usability, two key rules govern the VIP Network:

- If a company issues second-factor credentials to its end users, it agrees to allow those credentials to be used to authenticate for any member of the network.
- Any member of the network agrees to accept authentication credentials issued by any other member of the network.

In short, an end user who receives a credential from a member of the VIP Network knows that the credential can be used as a second factor at any site within the network.

#### *VeriSign Identity Protection Fraud Intelligence Network*

The VIP Fraud Intelligence Network is a set of shared services in the VIP Network that builds on the VIP Fraud Detection Service and helps businesses obtain intelligence about online identity fraud events happening outside of their enterprise.



Criminals on the Internet use many different mechanisms to capture personal information—including phishing Web sites, key loggers, false storefronts, and database theft. Often, criminals will try to use the same information on multiple Web sites, testing login information by trial and error, establishing multiple fraudulent accounts, or other malicious activities. In the offline world, because banks and credit card companies know that attackers will often reuse stolen identity information, they have established data-sharing consortia to identify fraudulent applications and account usage. The same approach can be used to stop identity theft and account fraud on the Internet.

VIP Fraud Intelligence Network leverages VeriSign's unique visibility into Internet threats, gleaned from the global operation of core Internet technologies, such as VeriSign® Managed Security Services and VeriSign® iDefense® Security Intelligence Services, as well as information gathered from other VeriSign partners. VIP Fraud Intelligence Network will leverage the emerging standards being developed in OATH to share transaction fraud or “thraud” information.

#### **+ VeriSign: A Trusted Partner**

The VIP Services and VIP Network are part of VeriSign's internet infrastructure. Billions of times each day, companies and consumers rely on VeriSign's Internet infrastructure to communicate and conduct commerce with confidence.

Today, over 91,000 Web sites across 150 countries display the VeriSign Secured™ Seal, allowing customers to confirm the identity of e-commerce sites. VeriSign is among the most trusted consumer brands for Internet security.

VeriSign's SSL solutions protect over 40 of the world's largest banks, 43 of the world's top 50 e-commerce sites, and 93 percent of the Fortune 500 companies.

VeriSign acts as a trusted third-party service provider for a diverse set of applications, ranging from providing intercarrier text and multimedia messaging, to supporting high-volume SMS voting for popular television programs.

VeriSign also operates many core services for the Internet and telecommunications networks—including the .com and .net domain registries—and SS7 telephone signaling networks, having processed as many as 30 billion queries in a single day.

The VeriSign operations staff has decades of experience in running critical infrastructure, keeping it secure and available. VeriSign monitors, manages, and protects the networks of many major financial institutions, utilities, government agencies, and other companies through VeriSign Managed Security Services.

Finally, iDefense Security Intelligence Services provide enterprises with the best original research on emerging threats and vulnerabilities. iDefense researchers monitor hacker forums in English, Russian, Chinese and other languages. This research is used to enhance VIP Fraud Detection Services.

All this experience and expertise is leveraged in the VIP Network. VIP Services are run by VeriSign, so you can be sure that they will be secure and reliable. No company can better protect you from fraud or your customers from identity theft.



### + Related Research and Development

Today, the VIP Services and VIP Network are an easy-to-use, comprehensive, low-cost, and intelligent package of authentication services. However, we are working on other initiatives to extend the VIP Services and VIP Network to provide even better identity protection.

#### *Mutual Authentication Services*

Multifactor authentication makes obsolete the attacks that are designed to capture end users' passwords, such as phishing, key loggers, and eavesdropping. Luckily, these are the most common attacks used by hackers today. However, man-in-the-middle attacks (such as wireless "evil twin" attacks) are growing more common and are likely to be a significant problem in the future.

VeriSign is continually working with browser vendors to make it easier for end users to distinguish legitimate businesses from imposters. The Extended Validation SSL (EV SSL) Certificate is a result of this research. EV SSL gives Web site visitors an easy and reliable way to extend their trust online. In Microsoft® Internet Explorer 7 (and upcoming releases of Firefox and Opera), the address bar turns green and displays the name of the EV SSL Certificate owner.

Additionally, VeriSign is working with standards groups like OATH to develop additional techniques for user authentication. As these become available, VeriSign intends to expand the suite of VIP services to help provide an even more secure experience for end users.

#### *Consumer Identity Management*

In addition to the need for user authentication, enterprises and consumers are still in search of a better solution to the identity management problem: As a consumer, how can I use the same "identity" on multiple Web sites, and how can I manage the private information that is shared with those sites? Can I access multiple Web sites with a single sign-on?

Research in this area includes work by Liberty Alliance (ID-WSF-2.0), Microsoft (CardSpace), Eclipse Foundation (Higgins), and OpenID. VeriSign Labs is a significant contributor to this research and has an OpenID implementation available at <https://pip.verisignlabs.com/>.

As these solutions complement fraud detection and strong authentication, VeriSign will continue to determine what new benefits can be gained by expanding the services of the VIP Network.

#### *Identity-Proofing Services*

When users initially register on a Web site, their identity must be validated. If they have no offline relationship with the Web site, this can be tricky. Identity thieves know this and often open accounts in the names of others. The FTC Clearinghouse survey has shown that over 20% of bank fraud, 60% of credit card fraud, and 95% of phone and utility fraud incidents involved creating new accounts.

Identity-proofing services provide a means by which a trusted third party can help confirm the identity of an end user or consumer to a Web site—a benefit to both parties.

This may be done online, via a series of questions relating to the registrant, or offline, via multiple sources and identity documents. VeriSign's experience as a Certificate Authority is relevant to this emerging opportunity, and VeriSign will continue to research ways to encourage the evolution of the VIP Network.



## WHITE PAPER

### + Learn More

For more information about VeriSign Identity Protection, please call +61 3 9674 5500 or email: [sales@verisign.com.au](mailto:sales@verisign.com.au)

### + About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

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



©2008 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

00025328 2-15-2008