



WHITE PAPER

# A GUIDE TO PROVIDING PROACTIVE PROTECTION TO CONSUMER ONLINE TRANSACTIONS



## CONTENTS

- 1 THE IMPACT OF CONSUMER “DIGITAL MIGRATION”
- 1 SUMMARY OF USER PROFILES
- 2 AUTHENTICATION FORM FACTOR USAGE TRENDS
- 4 VERISIGN IDENTITY PROTECTION
- 5 GLOSSARY
- 5 LEARN MORE
- 5 ABOUT VERISIGN





# A GUIDE TO PROVIDING PROACTIVE PROTECTION TO CONSUMER ONLINE TRANSACTIONS

## THE IMPACT OF CONSUMER “DIGITAL MIGRATION”

At an accelerating pace, consumers are doing more shopping and banking online for the convenience and choice that this experience brings. They are also taking more control and managing their healthcare accounts online. Finally, they are increasingly getting their news and entertainment content from online sources.

This digital migration has led to the evolution of business strategies for diverse industries, such as retail, financial services, media and entertainment, healthcare, and government services. For enterprises, the opportunity is the development of new distribution channels with the promise of increased sales and lower operating costs. Enterprises are challenged, however, by the need to deliver a differentiated online customer experience—which can drive customer loyalty—while combating fraud and its negative effects.

Weak user or consumer authentication has fueled the problems of Internet identity theft, including phishing and financial fraud. As more consumers do more online, the risk of fraud and identity theft increases and consumer fears are also elevated. In a recent survey conducted by Synovate Research for VeriSign, ten times as many consumers felt that trust is more important than cost when it comes to transacting business online.<sup>1</sup> This indicates that enterprises have an opportunity to differentiate themselves and stand to gain significant revenue by addressing the security and trust concerns of the online consumer.

Strong authentication for users has long been accepted in the enterprise as a technology to secure access to corporate networks and applications. However, technology that is suitable to the enterprise user population may not be the best fit for consumers. The hugely diverse consumer population dictates the need to segment users and apply the strong authentication technology that is the best fit.

1. Synovate Research conducted on behalf of VeriSign, October 2008.

## SUMMARY OF USER PROFILES

User populations that need access to enterprise network infrastructure can be roughly categorized into three segments: employees, business partners, and consumers. Each of these segments can be further divided by other characteristics related to the online experience. In selecting the best strong authentication solution, cost and the level of security risk can be balanced against providing the best online user experience.

### Employees

Employees represent a user segment that enterprise IT organizations are very familiar with. They are a captive audience to receive the proper training on whatever strong authentication technologies are deployed. Despite the fact that their usage falls into fairly predictable patterns, the following variations exist:

- Depending on the size and industry of an enterprise, some employees will be more technologically savvy than others.
- Employees with company-issued mobile phones represent a subsegment with different security needs and strong authentication solution options.

### Business Partners

In many ways, business partners are an extension of the employee population because their level of security and infrastructure access needs vary. Similar to employees, however, their access patterns are usually predictable and technologies are manageable.

### Consumers

On the other hand, consumers represent the most diverse user population—and the most challenging segment for enterprise IT organizations to manage.

- Many consumers (particularly in the younger demographics) are extremely comfortable with technology—both hardware and software. This includes users of mobile devices for Internet access as well as

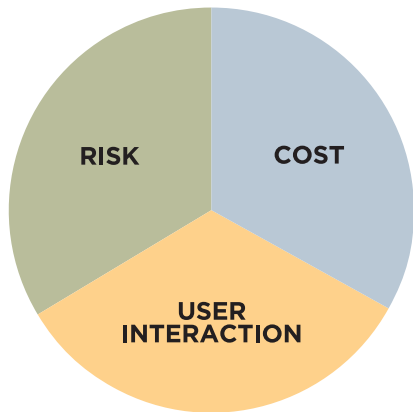




## WHITE PAPER

consumers who know the security advantages of using Microsoft Internet Explorer or Mozilla Firefox browsers.

- Other consumers are much more technology averse and may be comfortable only with using whatever browser or software comes preloaded on most popular consumer personal computers (PCs).
- The largest consumer segment (consisting of mid- to late-stage “baby boomers”) falls in the middle in terms of being tech savvy and its level of comfort with online business activity.
- Regardless of their level of comfort with technology, high-value or high-net-worth customers are also an important user segment because they are at higher risk of being targeted by online criminals and would benefit from added account security.



### BALANCED MANAGEMENT

Enterprises must take these user segments into consideration when selecting any consumer authentication solution. At the heart of the decision process is the balanced management of the risk inherent in each user segment, the solution cost, and the need to have user interactions that deliver a differentiated user experience.

The chart on the next page systematically illustrates how different authentication technologies can be mapped to the

most appropriate user segments. The chart also describes other key solution criteria in selecting an authentication technology, such as suitability to application, security level, costs, and intangible factors.

### AUTHENTICATION FORM FACTOR USAGE TRENDS

While there are no statistics from public, large-scale, authoritative surveys on consumer authentication technology adoption, anecdotal or public domain information does suggest some trends.

- With the size of consumer deployments, price sensitivity is a natural key factor—the one-time password (OTP)-only token form factor remains a popular choice in the EMEA (Europe, Middle East, Africa), APAC (Asia Pacific), and CALA (Central and Latin America) regions. It is also based on stable technology that has been available for the last 15 years.
- In regions like Europe and Asia where adoption of mobile-device technology tends to be on the leading edge, there is broad interest in mobile phone-based credentials (OTP implementation via Short Message Service [SMS] or mobile phone application).

---

### 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.”









“A nice product; I wish my own financial institution would institute.”

---






# WHITE PAPER

The chart below systematically illustrates how different authentication technologies can be mapped to the most appropriate user segments. The chart also describes other key solution criteria in selecting an authentication technology, such as suitability to application, security level, costs, and intangible factors.

Credential Types	Description	Security Level	Portability	Usability	User Profile	Support Costs	Unit Costs	Other Intangibles	Appropriate Applications
 <b>PKI certificates</b>	Small PKI certificate that sits on a user's machine	Excellent	Poor; exception is PKI certificates stored in hardware Universal Serial Bus (USB) devices, downside is that software drivers are required	Average/good; most users don't understand concept, MS browser interface is difficult to understand	Employee, business partner, and predictable computer accessing your network	Average/good; high costs due to lack of end user understanding and yearly lifecycle management	Average/good; cost of managing supporting infrastructure can be high. Very good; if outsourced		Any application requiring device authentication, Microsoft smart card logon, Virtual Private Network (VPN), business-to-business Web applications; any application requiring signing or encryption
 <b>OTP keyfob</b>	Convenient keyfob that's easy to carry and use	Very good	Excellent	Excellent	Employees, consumers	Average/good	Average	OTP credentials can be shared across multiple Web sites, branding opportunity high	Enterprise VPN, OWA, Web applications; Consumer: commerce, communities with private data
 <b>OTP tokens</b>	Small electronic device that generates a one-time password	Very good	Excellent; no connection required	Very good; dynamic password is an easily understood concept	Employees, consumers	Very good; low costs around usability, higher costs for distribution	Good	OTP credentials can be shared across multiple Web sites, branding opportunity high	Enterprise: Virtual Private Network, Open Workflow Alliance, Web applications; consumer: commerce applications, online communities with private data
 <b>OTP security cards</b>	Credit-card-sized credential embedded with an LCD to display one-time password	Very good	Excellent	Excellent	Consumers	Very good; low costs around usability and distribution	Average	OTP credentials can be shared; branding opportunity high; higher cost credential given newness in product lifecycle	Consumer: commerce applications, online communities with private data
 <b>Mobile credentials (software)</b>	Standalone application residing on phone, capable of generating a one-time password	Good	Very good; although new credential is required for new phones	Very good	Consumers, employees with enterprise-issued phones, tech savvy	Average/good during initialization Very good/excellent ongoing	Very good	OTP credentials can be shared; no distribution costs, leverages a device users already have	Enterprise: VPN, OWA, Web applications; consumer: commerce applications; online communities with private data
 <b>SMS OTP</b>	SMS-delivered one-time password to a user's handset	Good	Very good	Good	Consumers, tech savvy	Very good/excellent	Excellent	Gateway and carrier reliability/coverage is critical—low in U.S., high in Europe and Asia; data capability on phone necessary	Consumer: commerce applications; online communities with private data
 <b>Browser plug-in/desktop software OTP</b>	Browser plug-in client to generate one-time password	Average	Poor	Good	Employees	Very good/excellent for consumers; Average/good for enterprise-controlled distributions	Good	OTP credentials can be shared; requires client software to be deployed	Consumer: commerce applications; online communities with private data
 <b>Voice-enabled passcode</b>	Random passcode sent via voice call to user's handset	Good	Good	Good	Consumers, non-tech savvy	Very good	Good	Requires registered phone number and consumer access to that phone	Consumer: commerce applications; online communities with private data

CONTINUED NEXT PAGE



Credential Types	Description	Security Level	Portability	Usability	User Profile	Support Costs	Unit Costs	Other Intangibles	Appropriate Applications
<b>Secret questions/answers</b> 	Challenge questions/answers, e.g., mother's maiden name	Poor	Excellent	Average	Average; consumers often locked out	Average	Good	Requires cumbersome registration	Consumer: commerce applications; online communities with private data
<b>Images</b> 	Enabled by cookie sitting on machine of the user that interacts with a Web application to generate an image which was chosen/registered for by the consumer	Poor	Average	Good	Consumers	Average; consumers don't understand the purpose which can lead to faulty registrations, calls for clarification	Good	Easily phished	Consumer: commerce applications; online communities with private data
<b>Extended Validation SSL Certificates</b>  Identified by VeriSign, Inc.	Highly Authenticated SSL Certificate with an added benefit: It triggers select high-security browsers to display a shade of green in the URL	Excellent	Good; dependent on browser version	Very good	IE7 or higher	Very good; minimal to no support inquiries	Excellent	Minimal cost to provide encryption of data between site and user. Easily distinguishable interface enhancement for a large number of Web users.	Any Web site capturing personal and confidential data (user names, passwords, credit cards, national identifiers, etc.)

### VERISIGN® IDENTITY PROTECTION

Having the right credential to suit the user is only half the battle in trying to achieve consumer acceptance of strong authentication technologies. Users want a single “second factor” for different Web sites to avoid the need to have and carry multiple credentials.

What is needed is a solution approach that incorporates the idea of credential sharing for second-factor authentication. VeriSign® Identity Protection (VIP) is such a solution.

VIP supports a variety of two-factor authentication credentials, including security cards, software-generated credentials (e.g. mobile application and desktop toolbar), and RSA Security ID 700. VIP enables enterprises to provide a safe, easy-to-use, and trusted online experience for their consumers.

Credential sharing is enabled by the VeriSign® Identity Protection Authentication Network where credential issuers and relying parties can 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 enterprises to share the cost of a strong authentication infrastructure.

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

- **Ensures Freedom of Choice.** VIP supports a broad range of credentials including the RSA SecurID 700 keyfob offered by RSA, the Security Division of EMC. For vendor independence, VIP also supports any open-standards based (OATH) security credential.
- **Convenient and Simple.** Users have a single, portable credential (such as a keyfob token, credit card, or cell phone enabled for an OTP) that serves as a second authenticating factor for any VIP network site—similar to those used in ATM networks.
- **Cost Efficient.** VIP is a cloud-based authentication model in which VeriSign hosts infrastructure and Web services integration to minimize costs of deployment and shared maintenance. A consistent user experience also minimizes support costs for member sites.
- **Speeds Time to Market.** By delivering 2FA as a service, VIP makes it easy, fast, and cost-effective to offer strong authentication to customers. It speeds time to market, enabling companies to reduce fraud and increase revenue by building customer trust.





- **Trusted.** VeriSign has long been a provider of SSL 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.

## GLOSSARY

**Authentication** — The process of confirming that something is genuine. In computer security, authentication is usually an automated process of verifying the identity of someone or something, such as a computer or application.

**2-Factor Authentication, Strong Authentication, Multi-Factor Authentication** — All of these terms refer to the authentication practice of requiring confirmation of something you know such as a username and password and something you have such as a smart card, token or certificate.

**Credential** — Proof of qualification, competence, or clearance that is attached to a person. A digital certificate, token, smart card, mobile phone, or installed software are credentials that may be used to enable strong or multi-factor authentication.

**Extended Validation SSL** — Requires a high standard for verification of SSL Certificates dictated by a third party, the Certificate Authority/Browser Forum. In Microsoft® Internet Explorer 7, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

## LEARN MORE

For more information about VeriSign® VIP please call 650-426-5310 or email: [identityandauthenticationservices@verisign.com](mailto:identityandauthenticationservices@verisign.com)

## 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](http://www.Verisign.com) for more information.

