

WHITE PAPER

VIP ACCESS FOR MOBILE:

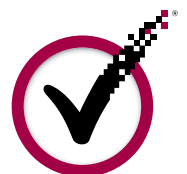
MAKING CONSUMER TWO-FACTOR
AUTHENTICATION SIMPLE AND
COST-EFFECTIVE





CONTENTS

- 1 INTRODUCTION
- 1 SOMETHING (NEARLY) EVERYONE ALREADY HAS
- 2 MOBILE CREDENTIALING BENEFITS BOTH CONSUMERS AND BUSINESSES
- 2 INTRODUCING VIP ACCESS FOR MOBILE
 - 3 CONSUMERS GAIN FREEDOM OF CHOICE
 - 3 MAKING 2FA AFFORDABLE
 - 3 A UNIQUE OPPORTUNITY FOR CARRIERS
- 4 TURNING SECURITY INTO AN OPPORTUNITY
- 5 CONCLUSION
- 5 GLOSSARY
- 5 LEARN MORE
- 5 ABOUT VERISIGN





VIP ACCESS FOR MOBILE: MAKING CONSUMER TWO-FACTOR AUTHENTICATION SIMPLE AND COST-EFFECTIVE

INTRODUCTION

Two-factor authentication (2FA) has proven itself indispensable as a highly effective means for corporations to protect their information assets. Now in wide use in many companies around the globe, 2FA is being wielded as a powerful weapon against multiple threats to an organization's information security.

Today 2FA is poised to become a mainstream security solution for online consumer transactions as well. Leading the industry in bringing 2FA to consumers is VeriSign—first with its shared authentication network, and now with its VeriSign® Identity Protection (VIP) Access for Mobile credential, a highly cost-effective and attractive complement to tokens, credit card-sized devices, and other forms of credentials.

By enabling the mobile phone to function as a secure credential for on-the-go, in the office, and at home online transactions, VeriSign eliminates any remaining hesitation on the part of companies or consumers about the convenience and cost of using 2FA. Now companies can affordably offer customers a choice of credential formats—including one that nearly every person on the planet already possesses—and in doing so appeal to the broadest swath of consumers possible.

Turning the ubiquitous mobile phone into a handy credential is an industry-shaping proposition that delivers a true win-win for all involved—companies with online services, consumers transacting business online, and mobile phone service carriers.

SOMETHING (NEARLY) EVERYONE ALREADY HAS

Consumers are skittish about online security, even holding back on conducting more business online until they have greater assurance that their confidential information and identity are safe. A report from the Federal Trade Commission showed that 61% of adult Americans are very or extremely concerned about the privacy of personal information when buying online.¹

2FA represents a giant leap forward in protecting consumers against online fraud. Today's consumers understand this and

are demonstrating in greater numbers that they are ready and willing to use 2FA for greater online security, even if it means carrying an additional item. Companies offering 2FA to their customers see that the benefits of building consumer confidence and reducing their fraud exposure outweigh the cost and effort of purchasing, distributing, and managing credentials.

Now there's a simple and incredibly powerful way to make 2FA even more convenient for consumers and cost-effective for businesses: the ubiquitous mobile phone.

Nearly everyone has one and they carry it with them everywhere they go—home, office, and on the road. The number of mobile phone users topped 3.3 billion at the end of 2007 according to the United Nations International Telecommunications Union²—that's half of the world's population. Enabling the mobile phone to serve as a credential eliminates the need for the vast majority of consumers to receive and carry an extra device.

STUDY SHOWS OTHER METHODS OF AUTHENTICATION INEFFECTIVE

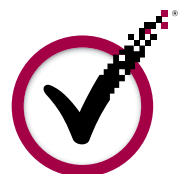
Researchers from MIT and Harvard studied the efficacy of measures such as authentication images to improve online security. These types of security systems rely on customers selecting an image that will always be displayed when they log into their account. The site authentication images are a cue for customers that the page they are viewing is in fact legitimate.

In the study, researchers watched 67 participants go through typical online banking activities. The site authentication images were removed to see how users would react. Of the 60 participants who completed the study, only two of them were suspicious about the image-less login pages and refused to log in. The other 58 signed on with little or no trepidation.³

1. "Consumer Fraud and Identity Theft Complaint Data, January-December 2007," The Federal Trade Commission, February 13, 2008

2. "Global Mobile Phone Users Top 3.3 Billion by End-2007," *Cellular-news*, May 24, 2008

3. "Study: Surfers Ignore Common Security Cues on Banking Sites," Eric Bangeman, *ars technica*, February 5, 2007





MOBILE CREDENTIALING BENEFITS BOTH CONSUMERS AND BUSINESSES

The evolution of the mobile phone dovetails neatly with the more widespread adoption of 2FA. Telecommunications, media, and information technology have converged recently to transform the mobile phone from a traditional voice communication machine to a multifunction personal device. Security is a natural extension of this trend.

Consumers have already embraced the fact that the mobile phone offers far more than wireless communications. Today's handsets deliver entertainment, communications, personal organizers, navigation, and many other desirable capabilities. Adding the ability to issue onetime passwords (OTPs) for strong authentication simply extends the versatility and usefulness of the mobile phone for consumers. It eliminates the need to carry an additional device and makes 2FA even more attractive and easy-to-use for consumers.

Businesses issuing credentials to their customers benefit as well. The business can now choose to offer a wide variety of credential form factors—with something to suit nearly every consumer's personal preference. A large jump in consumer uptake as a result of offering a convenient mobile form factor lowers costs and risks for all participants in a shared authentication network.

Mobile credentialing also offers the most cost-effective format for companies issuing credentials—eliminating the purchasing, shipping, and management cost and burden for credentials. It effectively lowers the cost of entry for businesses considering 2FA for their customers' transactions.

With a mobile phone as a secure credential, we can marry security and cost-effectiveness with convenience to deliver a significant impact on the industry—dramatically increasing uptake of 2FA capabilities to protect online transactions.

INTRODUCING VIP ACCESS FOR MOBILE

VeriSign created the foundation for consumer 2FA with a shared authentication network built around the idea of enabling one credential to be used on multiple Web sites. By leveraging the network effect, the shared network can reduce the cost and risk to participating companies of implementing a 2FA solution while offering a compelling value proposition to consumers.

Now VeriSign is combining the convergence opportunity of the mobile phone with shared authentication to accelerate adoption and drive costs lower for participating companies.

VIP Access for Mobile is a credential that runs on nearly all of the popular handsets used today. It enables consumers to obtain a one-time password (OTP) via their mobile phone for two-factor authentication on VIP network members' sites. In addition to on-device credentialing, VeriSign also offers an SMS alternative for flexibility.

By already supporting more than 60 different phone models, including the iPhone, VIP Access for Mobile ensures that the vast majority of customers can take advantage of mobile credentialing. The VIP Access for Mobile application is optimized for handsets, supports both J2ME and BREW, and features a very small footprint. Easily deployed on existing mobile phones, VIP Access for Mobile shatters the barrier to adoption—ushering in a new era of secure online transactions.

To read more about the network effect and a shared authentication network, download [“Leverage the Benefits of a Shared Authentication Network to Help Drive Consumer Retention and Strengthen Competitive Differentiation.”](#)



Figure 1. VeriSign VIP Access for Mobile Application



Consumers Gain Freedom of Choice

With VIP Access for Mobile, companies can now offer consumers the ultimate in convenience and security: using their existing mobile phone as a credential in two-factor authentication. As part of a blended approach—offering both mobile and more traditional credentials such as tokens or credit card-sized devices—companies can better serve the unique needs and preferences of their customers.

VIP Access for Mobile offers a mobile phone-resident credential application that circumvents latency, extra charges, and cell phone coverage limitations. Consumers experience no hidden charges when using VIP Access for Mobile to authenticate their identity for online transactions. And with the credential process resident on the mobile phone, consumers can still conduct online transactions in areas with no cell phone coverage.

Making 2FA Affordable

VeriSign® VIP Access for Mobile makes 2FA a cost-effective, affordable solution for nearly any company in any industry. It facilitates boosting consumer trust, reducing fraud losses, differentiating online offerings, and where relevant, complying with mandates such as the FACTA Red Flags rule.

VIP Access for Mobile eliminates the cost and organizational effort of creating, distributing, shipping, and managing mass quantities of tokens or smart cards. The VIP Access for Mobile credentialing application is simply downloaded over the air by the consumer or available pre-loaded on the phone's SIM card. It's a simple, easy to use, and highly cost-effective solution that will appeal to many consumers, encouraging broad adoption.

Issuers of VIP credentials retain all the benefits of distributing a branded credential. The mobile application, as well as the portal for downloading the application, offer full branding opportunities, including corporate logo and colors. Plus VeriSign offers flexible solution options that help further minimize deployment and maintenance costs:

Hosted by the VIP Network member

The front-end mobile application is built, hosted, and maintained by the VIP Issuer affording complete branding and control of the customer experience. VeriSign provides all the necessary APIs to communicate with both the delivery and the seed provisioning platforms to install the right application on the end-user handset and create the VIP credential.

Hosted at VeriSign

Alternatively, VeriSign provides a customizable, co-branded front-end to the VIP Issuer. VeriSign is responsible for building, hosting, and maintaining the front-end application, and only requires the phone number to be passed in the credential-provisioning process. No user-identifiable information is exchanged.

In both solution options, once the credential is provisioned successfully on the mobile handset, it becomes a credential in either the shared VIP network or the one owned and supported by the VIP Issuer.

A Unique Opportunity for Carriers

VIP Access for Mobile represents a strategic opportunity for carriers to create additional value to the consumer for their offering. Carriers can pre-install a carrier-branded VIP Credential on the handsets they offer, creating a competitive differentiator. For SMS-based VIP credentialing, the carrier also generates an adjacent revenue stream.



TURNING SECURITY INTO AN OPPORTUNITY

To illustrate the power and ease of use of VIP Access for Mobile, consider the following scenario:

A financial services company decides to participate in the VeriSign® VIP Authentication Network as a credential issuer. This company begins offering multiple forms of branded credentials including mobile phones and credit card-sized credentials to its customer base.

The financial services enterprise markets the increased security of its online services as a distinct advantage of its offering.

The company educates its customers on the value of 2FA and its ease of use. Consumers understand that the 2FA credential they receive from the financial services company can also be used to authenticate their identities to other Websites participating in the VeriSign® VIP Authentication Network.

Many of the company's customers adopt 2FA, selecting a credential form factor from the variety of those offered by VeriSign and the financial services organization. Figure 2 shows the broad range of credentials that VeriSign VIP supports.

The consumer enjoys both convenience and greater security. It's also the option with the lowest cost and level of effort for the company since there is no token or other form factor that must be purchased and deployed to the customer.

As 2FA adoption within the customer base spreads, customer confidence and trust is improved dramatically. More customers begin to take advantage of the company's online services, reducing operating costs. The drop in operating costs enables the company to be more competitive in its offerings to attract greater numbers of new customers.

Seen as a leader in its industry and a company that puts the safety and security of its customers first, the financial services organization now offers 2FA to each and every customer. Other companies in the financial services industry follow suit. Soon, consumers begin demanding 2FA for Web transactions in other industries such as healthcare and e-commerce. The ubiquitous mobile phone becomes the weapon of choice to fight cyber crime.

Figure 2. VIP Credential Form Factors



The mobile credential option is the most popular choice among the company's customers since it requires no additional physical item for the consumer to have on hand.





CONCLUSION

Many organizations have found that traditional deployment models for two-factor authentication present cost and scalability challenges when applied to the consumer market. VeriSign VIP Access for Mobile is the latest—and perhaps the most industrychanging—innovation that is bringing 2FA into mainstream consumer use.

Enabling the ever-present mobile phone to be used a credential sets the stage for mass adoption of 2FA while significantly lowering the costs for companies issuing credentials to their customers. Businesses can now seize the opportunity to make the Internet a safer place again for their customers—driving new revenues and building customer loyalty.

LEARN MORE

For more information about VeriSign® VIP Access for Mobile, please call 650-426-5310 or email: 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 for more information.

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.

