



WHITE PAPER

Leverage the Benefits of a Shared Authentication Network to Help Drive Consumer Retention and Strengthen Competitive Differentiation





CONTENTS

+ Introduction	3
+ Understanding the Network Effect	3
+ The Time is Ripe for an Authentication Network	4
+ Seizing the Opportunity	4
+ How a Shared Authentication Network Works	5
+ The Compelling Benefits of a Shared Authentication Network	6
+ Unique Advantages for Early Adopters	7
+ Conclusion	7
+ The VeriSign® Identity Protection (VIP) Network	8
+ Learn More	8
+ About VeriSign	8



METCALFE'S LAW: THE NETWORK EFFECT FOR COMMUNICATIONS

While the concept of the network effect was first presented back in the early 1900s by Bell Telephone, it was more recently popularized by Robert Metcalfe, a co-inventor of Ethernet. Metcalfe argued that the number of Ethernet card users needed to grow above a certain critical mass if users were to reap the benefits of their network.

Expressed mathematically, Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of users of the system (n^2). This law has been used to explain the network effects of communication technologies and networks such as the Internet.

Leverage the Benefits of a Shared Authentication Network to Help Drive Consumer Retention and Strengthen Competitive Differentiation

+ Introduction

People and companies around the globe benefit from the “network effect” every day—most without even realizing it. This powerful phenomenon is the driving force behind a number of innovations we now consider necessities. Formerly rare technologies and services such as the telephone, ATM machines, fax machines, e-mail, and Ethernet, have become ubiquitous because the value to all goes up as the number of participants in the network increases.

What if this concept was applied to the problem of protecting consumers from cyber crime such as identity theft, phishing, and fraud? Consumer use of stronger authentication such as two-factor authentication could finally achieve widespread adoption.

Visionary companies are recognizing that a shared two-factor authentication network is the strategic model that can overcome consumer security concerns while also driving user adoption. They realize that this is an entry point to enhanced customer loyalty, increased differentiation, and organic, profitable growth via online strategies.

The rewards for participating in a shared authentication network go far beyond what a single company could accomplish. Participants experience lower cost, less risk, increased protection against fraud, and greater success and acceptance of online offerings made safe for consumers through strong authentication.

This white paper introduces the concept of a shared two-factor authentication network, and discusses why a shared network for strong authentication is an essential requirement for continued customer participation in online interactions and commerce. It further explains how the network effect can help drive widespread consumer adoption of strong authentication, and the significant benefits available to organizations that choose to participate.

For more information about two-factor authentication, please download: [VeriSign Identity Protection Services Overview](#).

+ Understanding the Network Effect

The concept of the network effect has been recognized for at least 100 years, ever since the advent of the telephone. A classic example in more recent history is the automated teller machine (ATM). At first the ATM was limited to one card per bank. Users could withdraw cash and conduct other transactions only at ATMs at their own bank's locations. As ATM usage increased, interbank networks appeared enabling customers to use their ATM cards at any bank participating in the network. Today, ATM users can access their accounts from thousands of locations and the ATM card has become multipurpose, serving as a debit card, check cashing card, and other uses.

Mobile phones are another recent example of the benefits of the network effect. Providers understood that as the network of consumers with mobile phones grew, more people would see value in having one. As mobile phone usage approached a critical mass, service coverage increased and roaming charges began disappearing. Other revenue-rich examples of the network effect include email, instant messaging, and even the Web itself.

“The shared Network concept addresses two key drivers that will help drive widespread adoption of consumer authentication: convenience and ease-of-use to consumers. This gives consumers a convenient and easy-to-use solution to address their concerns of identity theft with the use of the same credential across many Web sites. In addition, enterprises establish trust with their users without having to shoulder the entire burden of deployment and development costs.”

—Sally Hudson, IDC

A non-technology related example is the airline hub-and-spoke model. This model provides travelers with greater choices of destinations. As more people choose these destinations, more routes are made available, further increasing the convenience to travelers, while also providing greater service opportunities for the airlines.

This same concept of the network effect can be developed and applied for significant benefit to businesses participating in a secure authentication network based on two-factor or strong authentication. With wider consumer adoption and greater consumer confidence, companies participating in the network experience new branding opportunities, improved customer loyalty, and lower security risk and cost. Savvy companies are seeing these benefits and reaping the reward of early adoption now.

+ The Time is Ripe for an Authentication Network

As of March 31, 2008, there were 1.4 billion Internet users¹ surfing the Web worldwide. These online consumers exchange email, participate in social networks, book travel, download music, shop, and much more. While the Internet has radically transformed the way people live, work, and play, the potential to leverage the Internet for ever more innovative business applications is still far from saturated.

Today, security is threatening to inhibit online growth and innovation. From phishing to malware, the Internet is literally teeming with criminals wielding an arsenal of weapons to defraud consumers and businesses. A recent report from the Federal Trade Commission showed that for the eighth year in a row, identity theft was the number one consumer complaint.²

Trends show that criminals are no longer targeting only financial institutions. Online retail, healthcare, transportation, and many other industries are now fair game as cybercriminals look for ways to diversify and become more sophisticated.

+ Seizing the Opportunity

No security solution can be effective if consumers aren't using it. While two-factor authentication delivers the enhanced security needed to combat cybercrime, uptake has been slower than desired. Data indicates that consumers are reluctant to maintain multiple credentials for the myriad of Web sites they frequent.

This seeming barrier to adoption provides the crux of what is perhaps the most innovative and consumer-friendly solution to security on the Internet: the shared two-factor authentication network. Businesses share a trusted authentication infrastructure, and consumers are able to use a single security credential to authenticate their identity across any Web site in the network.

A shared authentication network delivers an extremely user-friendly and effective method of two-factor authentication that encourages and rewards consumer adoption with the use of a single credential across multiple Web sites. It enables shared two-factor authentication to be both easy to use (regardless of the consumer's level of technology sophistication) and convenient for consumers.

¹ www.internetworldstats.com, Miniwatts Marketing Group

² “Consumer Fraud and Identity Theft Complaint Data,” January-December 2007, The Federal Trade Commission, February 13, 2008

In a survey conducted by VeriSign at the eBay Live conference in June 2007, responses showed that PayPal customers are very interested in using a shared two-factor authentication credential (token in this case), for other sites they visit on the Internet. In fact, 84% said they were interested in using the token at their bank, 52% wanted to use the token at their broker, 49% expressed interest in using the token for healthcare purposes, and 67% wanted to use the token for other transactions such as online shopping or gaming.

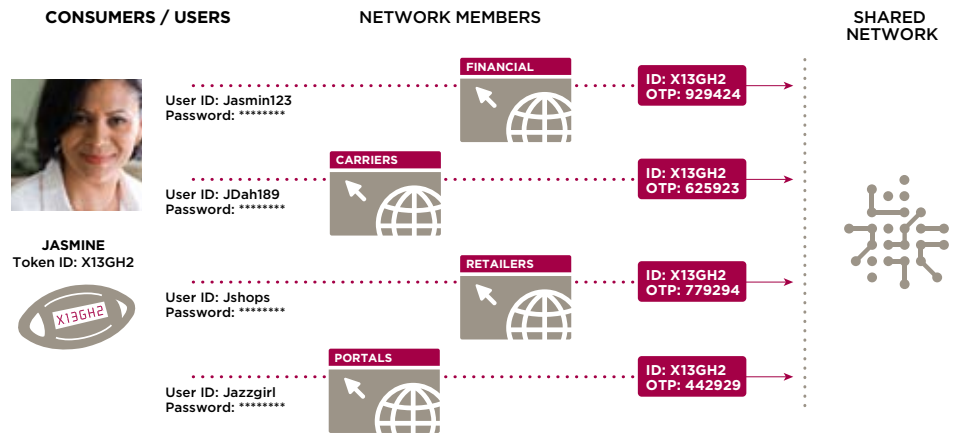


+ How a Shared Authentication Network Works

With a shared authentication network, instead of using a different credential for each online account, consumers have one credential for secure access to any Web site that displays the network logo or identification. The consumer's identity and transaction information stays within the participating company's system; only the security code or one-time password (OTP) and the credential ID passes anonymously to the shared authentication host for validation. This allows businesses to continue to control their customers' online experience while enhancing security with strong authentication.

Figure 1 below shows how a consumer interacts with businesses participating in the network. The same credential is used to deliver strong authentication for the consumer's identity across the various Web sites the consumer interacts with. At the same time, authentication by the network host is transparent to the consumer.

Figure 1: Consumer Experience with a Shared Two-Factor Authentication Network



Further, having a network of participating companies enables fraud intelligence and security experiences to be shared instantly across the network, increasing the security of each individual business and the network as a whole.

The network model also permits variations in the way companies participate. Network members can simply accept credentials issued by other network members and reap the many benefits of network participation. On the other hand, organizations can be offered the opportunity to issue credentials. These credentials, in the form of tokens, a text message sent to a mobile phone, or a credit card, for example, could be branded—giving the brand owner greater exposure to its customer base and beyond.

+ The Compelling Benefits of a Shared Authentication Network

For consumers, shared authentication offers the safe haven they need to feel confident about Internet usage and online commerce. They gain greater security without having to sacrifice convenience. And as more sites participate in the network, the value of the security solution increases over time for each consumer, which then drives further adoption.

With a shared authentication network, the lion's share of the cost, risk, and effort required to ensure continuous levels of strong authentication is spread out over many companies. Similar to the advantages of software as a service (SaaS), participating companies in a shared authentication network don't have the upfront capital investment associated with an in-house solution. As a hosted solution, there is no software to install and maintain, no additional hardware required, and no support or maintenance burden. Scalability and reliability are ensured by the host of the shared network.

Network members retain control of the customer experience, while benefitting from cost savings and greater acceptance of the solution from customers. Avoiding custom development enables organizations to speed the time-to-market for more secure services and offerings. And these benefits increase as more and more organizations join the network, effectively amortizing costs.

Beyond the cost and effort savings of a shared authentication network, it also offers unique branding and revenue-sharing opportunities to companies participating as credential issuers. These companies can ensure that their brands are in front of their customers each and every time they visit the Web. And the brand exposure does not stop there. Companies participating in the network experience greater exposure outside of the customer base, as consumers with credentials from other issuers visit their sites.

For those network members who are issuing credentials, revenue-sharing can help offset a portion of the service cost. Each time credentials from the issuer are activated by relying parties, the issuer receives a share of the fee paid.

A Shared Authentication Network: From Initiation to Maturity

In a sample scenario, an online auction site is aware that growth in customer transactions has slowed due to security concerns. Data indicates that offering two-factor authentication is perceived as a value-add by a segment of its high net-worth users. However, data also indicates these users want the convenience of using a common credential across multiple sites. With a reasonable initial investment, the auction site joins a shared two-factor authentication shared authentication Network, and additionally selects to be a credential issuer to take best advantage of brand opportunities with these high-value customers.

While initial adoption within the high-value user segment is brisk, the organization is pleasantly surprised when adoption migrates into other customer segments as well. As other sites join the network, the network logo becomes more widely recognized, with more and more of the auction site's users seeing the value of the common credential. The site is also pleased to realize a revenue increase as its branded credentials are used on other participating sites.



The number of companies participating in the network continues to grow, offering more opportunities to consumers for strong authentication, while maintaining convenience. Consumers are now becoming reluctant to use sites that are not part of the shared network, organically locking in loyalty and creating opportunity for more transactions with participating companies. Overseas customers are attracted to the network's increased security and begin transacting on the auction site, effectively extending the site's geographic reach. It begins up-selling additional services to its credential holders.

As the network's critical mass is achieved, virtually all the auction site's users now want two-factor authentication. The company is seen as a leader in consumer security and state-of-the-art fraud protection. It has increased its presence across other network members' sites and receives a share of the revenue from the network provider for accepting credentials from other issuers on its Web sites. The auction site's branded credentials are used at thousands of participating sites every day. Customer loyalty and transactions are up, and the credential relationship offers a valuable channel for future branding, selling, and service opportunities. Satisfaction is high and the number and cost of fraud-related incidents has been reduced. The full benefit of the network effect has been realized.

+ Unique Advantages for Early Adopters

Why be the first on a shared authentication network? There are distinct benefits awaiting those companies joining the network as early adopters. These advantages go above and beyond the effective, scalable, and reliable strong security solution it provides. Participating in a shared authentication network early in its lifecycle establishes competitive differentiation, positions the company as an industry leader, and garners positive media coverage for introducing innovative security solutions. For companies seeking international market share, it attracts potential customers from countries where consumer shared two-factor authentication is already a respected, well-known solution.

+ Conclusion

A shared authentication network elevates two-factor authentication from a pure security measure to a strategic business opportunity. The benefits created by a shared authentication network go far beyond allaying security fears and protecting the bottom line—participation can be a launch pad for differentiated, innovative online offerings.

Any company with an online account management application today or considering one in the future should learn more about shared two-factor authentication and the advantages of the network effect. They should then use that knowledge to develop a strategic model that will help to shape the future of Internet usage and establish competitive leadership in delivering a secure, online experience.



+ The VeriSign® Identity Protection (VIP) Network

VeriSign® Identity Protection (VIP) Services help your consumers conveniently and securely log in to their accounts to use your online services. Two-factor authentication, self-learning fraud detection, and a powerful validation infrastructure help provide a secure end-to-end solution at a reasonable cost from the most recognized trust brand on the Internet.

Enterprises who are VIP Network members benefit from the network effect of a single, in-the-cloud validation infrastructure and global intelligence. Consumers, who conveniently use one credential to log-in to multiple web sites, have the added protection of second-factor authentication. The VeriSign® Identity Protection (VIP) Fraud Intelligence Network provides early warning of attacks and comprehensive watchlists to block potential fraud sources.

+ Learn More

For more information about VeriSign Identity Protection, 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.