Abstract

As more financial and commercial activity move online, businesses are seeking to bolster consumer security and confidence. In a 2007 report, Forester notes that thirty-seven percent of online shoppers concerned about identity theft have stopped buying online altogether, leading to an estimated loss of $40 billion in online sales. Gartner, in a 2008 report, reveals that most consumers consider security features extremely important factors that influence their decisions to bank online and do more online business with their bank.

In other sectors such as higher education and healthcare, where patient records and student data need to be protected, the significant benefits of online services could be forfeited due to data protection and user confidentiality concerns. Industry leaders and consumers alike recognize that there is a real need for stronger authentication to protect digital resources and alleviate consumer concerns about the risk of doing business online.

In this white paper we take a look at how strong authentication can benefit eCommerce and online services. We will evaluate the risks that identity fraud, phishing and cybercrime pose for online service providers, and discuss how strong user authentication can alleviate these risks by increasing consumer confidence and protecting digital identities and resources.

2. Gartner, Inc. 28 May 2008 ID Number: G00158229 Banks Need to Strengthen User Authentication while Appeasing Consumers
# The Future of Authentication for Online Services

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Securing Online Services with Strong Authentication</td>
<td>5</td>
</tr>
<tr>
<td>New Trends in Authentication</td>
<td>6</td>
</tr>
<tr>
<td>Strong Authentication Solutions Best Suited for Online Services</td>
<td>8</td>
</tr>
<tr>
<td>SafeNet Authentication Solutions for the Online Services Market</td>
<td>9</td>
</tr>
<tr>
<td>Summary</td>
<td>11</td>
</tr>
</tbody>
</table>
Introduction

Conducting business online has become a critical element of the world economy. As stated pertinently by the CSIS Commission on Cybersecurity for the 44th Presidency, “The use of Cyberspace has become a central element for many companies’ business plans - how they manage their supply chains and their internal services and how they work with their customers.”

With US online spending expected to reach approximately $144 billion in 2010, the e-commerce market in particular offers huge business potential for consumer facing industries.

Online Services: The Forces in Action

**Increased Risks**
- Static Phishing
- Dynamic Phishing – MITM attacks
- Trojans / MITB

**Costs & Efficiency**
- Identity proofing
- Provisioning and distribution
- Help Desk

**Legal & Compliance Need**
- Regulatory pressure
- Privacy
- Digital Signing

**User Experience & Customer Acquisition**
- Roaming
- Ease of Use
- Multiple Service Providers

**Increased Risks for Online Business**

While doing business online has become an integral part of our daily lives, there has also been a sharp increase in cybercrime, which has dampened consumer confidence and resulted in severe financial losses.

In the not too distant past, cybercrime was motivated more by the technical challenge of breaking into computer systems and was perpetrated by amateurs. No more. Today, cybercrime is being carried out by highly sophisticated criminals who are motivated by financial gain. This trend is reflected in numbers: a survey by Gartner, Inc, in 2007, reveals that $3.2 billion was lost to phishing attacks in the United States alone. One of the most sensitive industries to online security breaches is the financial services sector: companies in the financial services sector were the most targeted for phishing attacks in the last quarter of 2008.

---

4. U.S. Online Retail Forecast, 2005 to 2010, Juniper Research, Patti Freeman Evans
5. Anti-Phishing Working Group, March 2009
Businesses and organizations that want to realize the potential of online services and ecommerce, as well as consumers, recognize the need for more stringent security measures and authenticating users in the online environment.

The Problem with Passwords

The use of usernames and passwords has been the most common method for authenticating users who want to access online resources and services. But passwords, to a large extent, have been a victim of their own success.

**Too Many Passwords:** According to a BBC Click Online News Report, the average person holds approximately 20 different online accounts for online banking, internet-based mail, social networks, online retailers and more. Although one password may be easy to remember, handling many passwords is counterproductive since in order to remember multiple passwords users write them down, compromising the very security they were supposed to provide.

**Passwords are easy to share:** Companies have very little way of ensuring that users don’t share their credentials and passwords with colleagues, friends — and in extreme cases — criminals.

**Passwords are expensive:** In order to make passwords more effective, many organizations have imposed more complex password policies. But complex password policies increase the likelihood that users will forget their password, requiring a call to a helpdesk. Such calls drive up the cost of IT support and reduce productivity.

**Passwords are not secure:** To handle multiple credentials, users often choose passwords that are easy to guess, use the same password for several accounts, or write down passwords and store them where they are easily found. In addition, passwords are subject to social engineering attacks where thieves use scams to convince people to disclose passwords. Adding to these risks, many tools are available that can “crack” a password using “brute-force” attacks that attempt combinations of the accepted character set in order to find the one that provides access to the authorized area. These attacks are very efficient, accessing a seven-character, lower case password in as little as four hours.

Legal and Compliance Pressures

One of the forces that are increasingly affecting organizations and businesses operating in the online environment is the rise in the number of regulations that have been initiated by government agencies and industry bodies. As of November 2008, 44 US states had enacted laws requiring notification of security breaches involving personal data, according to the National Conference of State Legislatures. Other government and industry requirements, such as HIPAA and the Payment Card Industry Data Security Standard (PCI DSS) also mandate that companies secure their customers’ sensitive information.

The goal of these regulations is to create a standardized approach to issues including privacy protection, identity theft and data protection. As a result, many businesses and organizations are increasingly obliged to comply with various regulations when operating in certain sectors.
Examples of regulations include:

EU Directive on Data Protection (Directive 95/46/EC): Protects individuals with regard to the processing and transfer of personal data throughout the European Union

U.S. Senate – introducing legislation to protect consumers from ID theft: For example, the Identity Theft Protection Act – requires entities that collect sensitive data (e.g. social security numbers) to secure the data, and notify consumers when the data is compromised

U.S. Federal Deposit Insurance Corp (FDIC): Direct financial institutions to upgrade their customer authentication systems from single-factor to two-factor

KISA (Korean Information Security Agency): Regulations issued by the Korean Information Security Agency aimed building a safe and reliable cyber world by fostering trust through electronic signature certification, the protection of IT infrastructure and establishing a global security evaluation scheme for security systems & products.

Securing Online Services with Strong Authentication

Given the centrality of online services to our economy, it is essential to find ways of ensuring the integrity of our digital resources, preventing identity fraud and securing our online environment. Strongly authenticating users by validating their identities when they access an online service is key to enabling the online economy. With strong authentication, the online economy can flourish by:

- Enabling new services for employees, guest workers, business partners and customers
- Addressing associated risk and compliance issues by protecting customer information, financial data, healthcare records and mission critical applications
- Increase productivity by enabling more applications and services to a wider pool of users

What is Two-Factor Strong Authentication?

Strong authentication solutions enable organizations to ensure that a user is indeed who he or she claims to be. They increase the security of the authentication process beyond passwords by requiring two or more of the following forms of authentication:

- **Something you know** – something the user needs to remember, such as a password, a PIN, or an answer to a personal question
- **Something you have** – something the user needs to physically possess, such as a token or a card
- **Something you are** – a biometric feature, such as a fingerprint or facial characteristic
Strong authentication solutions commonly involve a physical device – ‘something you have’ (e.g. a token), used together with a password – ‘something you know’ – to prove the owner’s identity. A wide variety of strong authentication token technologies and form factors are available and are currently being used in the market:

- **USB Tokens**
  USB tokens are small handheld devices that users connect to their computers’ USB ports in order to authenticate. Users are granted access upon plugging the token into the USB port and entering the token password. The physical connection between the token and the computer enables these tokens to be used for multiple security applications such as secure local and remote network access, Web access, laptop and PC protection, file encryption, user credential management, and secure transactions.

- **Smartcards**
  Smartcards are credit card-sized devices that contain highly secure microprocessor chips dedicated for cryptographic operations. To authenticate, users must insert their smart cards into their readers and enter a password. Smart cards provide highly secure storage of user credentials and keys. They also secure PKI implementation by generating keys and performing cryptographic operations on-board, without ever exposing the user’s private key to the computer environment.

- **Smartcard-based USB Authenticators**
  Smartcard-based USB authenticators, which contain a smart card chip leverage the advantages of both USB tokens and smart cards to provide the greatest level of security and versatility. They enable a broad range of security solutions and provide all of the benefits of a traditional smartcard and reader — without requiring the separate reader.

- **One-time Password (OTP) Authenticators**
  OTP authenticators are small handheld devices that allow authentication using onetime passwords generated by the device, based on a secret key shared by the device and an authentication server. A user wishing to authenticate enters the one-time password appearing on the token, and this value is compared to the value generated by the authentication server. While OTP tokens are highly portable, they do not provide the same level of support for multiple security applications that USB tokens and smart cards offer.

- **Hybrid Authenticators**
  Hybrid authenticators provide multiple types of functionality, which increases flexibility. Hybrid USB and OTP tokens allow full USB-based strong authentication and security solutions, as well as OTP-based strong authentication in detached mode when needed. Smartcard-based hybrid tokens that use the smart card chip for both USB and OTP functionalities provide maximum security.

### New Trends in Authentication

Beyond the strong authentication methods mentioned above, over the past few years there have been innovations in authentication that open up the playing field to more flexible and diverse solutions.

#### Mobile Out of Band Authentication Solutions

Out of Band Authentication (OOB) is based on the two-factor authentication model but utilizes a combination of software authentication together with separate information channels for authentication and access. OOB methods leverage the one device users already have, such as a mobile phone, handheld device or PC, in
order to generate passwords that facilitate authentication. Examples of OOB authentication include authentication via SMS, where an SMS is sent to a mobile phone for authentication, a voice callback to a phone for authentication or software-based authenticators which are generated by software that resides on a mobile phone.

While very convenient and cost effective, OOB authentication methods are not as secure as traditional two-factor authentication methods. OOB methods are also dependent on mobile network coverage for the delivery of passwords to mobile devices. Lack of coverage can result in delayed delivery or delivery failure.

**Readerless USB Authenticators**
Readerless USB authenticators are an innovative form of USB certificate-based authenticators that, unlike regular USB certificate-based authenticators, do not require middleware on the end-user computer. Readerless USB certificate-based authenticators offer the security of PKI technology with a much higher level of convenience and portability since they can be used on any computer that has a USB port and Internet connection.

**Software Authenticators**
Software authenticators enable strong authentication without a dedicated physical device. These tokens are software applications that can be stored on a user’s computer, or on mobile devices such as a cellular phone or PDA. Software authenticators can utilize either PKI (certificate-based) or OTP technology. They can also be used with mobile devices. While software authenticators are convenient for users, they are less secure than physical tokens because the secret key can be stolen or misused relatively easily.
The online services environment poses challenges for the implementation of authentication solutions. Unlike an enterprise-type environment, the world of online services is a business to consumer environment where there is very little control over the end-user setting. For this reason, several factors need to be addressed when assessing the selection of an authentication solution. These include:

- User mobility and ease-of-use
- IT and support issues
- Compatibility with end-user systems
- Security level required
- TCO constraints

**User Mobility and Ease-of-Use**

End-users in the consumer and online services market vary greatly in their levels of technical know-how and use habits. Moreover, in this type of uncontrolled environment, it is impossible to know what computers, drivers, operating systems or networks are being used to access protected resources.

A basic tenet of use-cases in the online environment is that users are mobile and do not necessarily use the same access computer for each online session. Authenticators need to strike a balance between acceptable security levels and portability.

**IT and Support Issues**

In uncontrolled mass user markets such as ecommerce, education, finance, healthcare or gaming, where thousands of end-users are involved, it is important for organizations that deploy strong authentication to be able to minimize help-desk costs provide simple solutions for customers who lose their tokens.

**Deployment and Management**

Organizations deploying large numbers of tokens in an uncontrolled environment need to take into account logistical efficiency issues such as deployment, distribution provisioning and support. They need to be able to centrally manage a large number of tokens and offer solutions for customers who lose or misplace tokens.

**Level of Required Security**

A significant factor determining what kind of authentication solution to deploy relates to the level or strength of authentication required vs. user mobility. The level of security required for online banking is usually more robust than that required for access to Web-based student email, for example, and online service providers should take into account the specific needs of the online service provided when choosing a solution or combination of solutions. The graph on the next page shows how various solutions reconcile user mobility and ease-of-use with authentication strength.
The Future of Authentication for Online Services

User Mobility vs. Authentication Strength

Low Total Cost of Ownership

Not only have purchase prices for strong authentication solutions fallen to affordable levels, available solutions also offer low TCO costs. Because users only need to remember a single password, they are less likely to forget their password, thus minimizing the cost of password management. A strong token management system also makes it faster and easier—and less prone to error—to manage the token life cycle and to replace lost or stolen tokens so mobile users remain productive.

SafeNet Authentication Solutions for the Online Services Market

SafeNet authentication solutions enable business value for online service providers and organizations looking to provide remote users (customers, partners, internal users) with strong, secure access to online Web services, and digital signing capabilities on a platform that is intuitive and easy to use.

SafeNet’s broad range of plug & play clientless and software-based authentication solutions are ideal for vertical markets such as banking and finance, trust centers, healthcare, education, and government agencies. SafeNet’s solutions strike the ideal balance between strong security and ease of use by enabling secure, convenient access for thousands of users anytime, anywhere without the need for client software.

Complementing our range of authenticators, SafeNet offers eToken TMS - life-cycle management software - that facilitates the central management, deployment and provisioning of tokens to large numbers of users. TMS offers tangible benefits to organizations and businesses carrying out mass deployment of authenticators as it reduces management, helpdesk and overhead costs considerably.
### SafeNet authentication solutions that are best suited to the Online Services market:

<table>
<thead>
<tr>
<th>Product</th>
<th>Online Services (consumer, healthcare, finance, education)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SafeWord 2008</td>
<td>SafeNet’s simple to deploy and easy to use SafeWord solutions enable small and medium businesses to quickly set up strong authentication for network access in a matter of minutes. SafeWord packages are ideal for Windows environments, offering seamless integration with Microsoft Active Directory.</td>
</tr>
<tr>
<td>eToken PRO Anywhere</td>
<td><strong>eToken PRO Anywhere</strong> is a roaming USB authenticator that enables secure access to the Web, authentication applications, digital signatures, encryption, decryption, and secure e-mail easily, conveniently and most of all, securely, from any computer. It does not require installation of any software on the access computer, making this a highly secure and portable device.</td>
</tr>
<tr>
<td>eToken TMS (Life Cycle management)</td>
<td><strong>TMS</strong> is a central fully configurable management platform that links security devices with users, organizational rules, and the associated security applications in a system. TMS enables centralized control of all authentication devices, for seamless deployment, administration and user management.</td>
</tr>
<tr>
<td>Software Authenticators</td>
<td>SafeNet offers both certificate-based and OTP software authentication solutions that combine the security of proven two-factor authentication with the convenience of authentication via a personal mobile device or PC.</td>
</tr>
</tbody>
</table>
Summary

In today's business world, online services - banking, e-commerce, enterprise portals, government services and medical consulting - are a significant part of mainstream economic activity. But parallel to the rise in online business, there has been a sharp increase in cybercrime.

To enable new business opportunities and to protect data and identities, stronger user authentication has become a critical component of a holistic security program. Strong authentication solutions boost productivity by allowing partners and employees to securely access business applications in the office, at home, or on the road, and provide a secure way for customers and users to access their private accounts and carry out transactions online with the confidence that their digital identities and personal information is safe.

In the uncontrolled online services environment, clientless authentication solutions that facilitate user-roaming and mobility, convenience and ease-of-use are growing in appeal. Clientless certificate-based solutions combine ease-of-use, while simultaneously providing more secure levels of strong authentication than other methods. Certificate-based solutions are also relevant for services that require digital signatures to complete transactions. Other innovative authentication developments, such as utilizing mobile devices for out-of-band and software based authentication solutions which leverage the ubiquity of mobile phones and PDAs, are attractive and likely to grow in popularity.

Given this wide-reaching range of available authentication solutions, it is becoming easier on the part of businesses, federal agencies and consumer-facing organizations to select the method that best suits their particular needs. Among end-users too — whether they are doctors, online shoppers, students or federal suppliers — there is a growing willingness to accept the additional step of user authentication when accessing online services in order to protect themselves from the dangers of identity theft and fraud.