# Hardware and Software Authentication: Choosing the Right Approach

**DECISION GUIDE**

## Table of Contents

## Executive Summary

To support today's organizations, IT departments need to foster the productivity of remote and mobile users, while safeguarding the security of sensitive assets and systems. For these reasons, strong authentication mechanisms are increasingly being employed. This paper compares the strengths and weaknesses of hardware- and software-based authentication approaches, and offers five key considerations for evaluating which approach is right for the specific needs of your organization.

## Introduction: The Changing Nature of Remote and Mobile Access

For years, organizations have been undergoing a transition in the nature of remote and mobile access. In the past, a user outside of the corporate office simply couldn't access email or any other business applications or data. Over time, Web-based email, VPNs, online portals, and an array of other technologies have opened up corporate resources to those outside of the brick-and-mortar office. Today, it is quite simply a competitive mandate to deliver the same tools and services to authorized users, whether they are inside or outside the four walls of an organization.

In fact, today, the line separating internal and external users is growing ever more blurry. Here are just a few of the reasons for this:

- **Mobile workers.** For outside sales organizations, customer-facing executives, consulting teams, and a host of other employees, optimizing productivity is a competitive mandate, whether those users are in an airport, hotel, customer site, home, or anywhere in between. For sales, mobile access is essential, which is why most enterprises continue to focus on better equipping mobile sales teams. For example, according to Gartner, more than 55% of Global 2000 organizations will deploy mobile sales force automation projects by 2011.
- **Smart phone and social network ubiquity.** With the combined, widespread adoption of smart phones, social networking, and advanced phone-based apps, the shifting lines between corporate and personal use, as well as authorized and unauthorized device use and access, conspire to make policy definition and enforcement increasingly difficult.
- **Teleworkers.** Providing effective remote access to employees who telecommute from a branch or home office is increasingly a must have for organizations. Today, approximately 90% of large enterprises worldwide have remote workers. The business justifications for doing so are many: With increased telecommuting, organizations can save on facilities costs, boost employee productivity and morale, and strengthen recruitment efforts by offering this perk. Further, employees can enjoy time and cost savings by reducing their time commuting, and gain greater flexibility, particularly given the increasingly global nature of business and the common need to work with partners, customers, and colleagues across multiple time zones.
- **Online transactions and services.** Today, consumers increasingly expect to do virtually anything online with their vendors that they could do in person, whether that means doing online banking or trading, selling goods or services through portals or online auctions, or a host of other transactions. For the businesses in these markets, delivering online services is a fundamental requirement for doing business.
- **Outsourced services.** Whether it's an offshore contact center, a third-party manufacturing or development team, or a host of other organizations, businesses are increasingly reliant upon external partners and vendors. Supporting these organizations with timely, reliable access to corporate systems and applications is one of the keys to making these relationships successful.
- **Disaster response.** In the event of natural or man-made disasters, or evacuations due to the threat of these occurrences, the loss of user productivity can exact a large toll. One of the key ways organizations can mitigate these losses is to foster worker productivity from outside corporate offices..

## Remote Access: The Security Implications

Businesses must balance the needs of shareholders, auditors, employees, customers, and a host of other constituencies. Toward that end, security is always something of a balancing act. Rigorous security mechanisms can't be broadly deployed if they unduly hamper end user productivity. Likewise, new productivity-enhancing applications can't be broadly employed if they present security threats or compliance issues. Finally, in almost any organization today, the issues of up-front cost and total cost of ownership are big considerations—meaning any significant security investment will receive intense management scrutiny.

Perhaps nowhere is this balancing act more evident than in the area of securing the identities and access of remote users. Given the proliferation of the types of remote access outlined above, organizations have had to balance the business mandate of enabling convenient, reliable remote access, while ensuring identities, sensitive data, and business-critical systems are secured. For each type of remote access granted, a new series of security threats is brought into play. When consumers can do a host of online banking transactions, the theft of passwords becomes a ripe target for criminals. When employees are able to gain access to sensitive internal resources from home, organizations can be even more exposed to theft and destruction of corporate assets by malicious employees. And the list goes on.

### The Limitations of Traditional Approaches

Over the years, IT organizations looking to secure remote access have confronted a number of difficulties:

*Strong user authentication has been an increasingly essential component of the security framework—a vital means to ensure that users, no matter where they are, are in fact who they claim to be and are authorized to gain access to business services.*

**Limitations of remote access gateways.** Remote access gateways, such as VPNs, Citrix, and Outlook Web Access, all create secure tunnels over the Internet. These gateways provide a convenient and secure remote link to network resources. However, relying on simple user names and passwords to access the entrances to these secure gateways is similar to leaving the front door to your house unlocked, or using a lock that can be easily picked.

**Exposure of passwords.** Static passwords are an unreliable mechanism for guarding the entrance to your trusted systems, applications, and networks. Many passwords can be easily guessed, hacked, or compromised by brute force attacks.

**Challenges of complex password policies.** Even complex password policies present problems for end users and IT departments. For example, changing passwords every 30 days, not allowing users to repeat a password over a given time period, and requiring multiple special characters in passwords adds significant complexity. Users may simply forget their password, requiring a call to the help desk to reset the password, which can increase the overall cost of IT support and lost productivity, to say nothing of diminished user convenience.

## The Need for Strong Authentication

Given the limitations and threats outlined above, strong user authentication has been an increasingly essential component of the security framework—a vital means to ensure that users, no matter where they are, are in fact who they claim to be and are authorized to gain access to business services.

Strong authentication—also known as two-factor authentication—refers to systems that require multiple factors for authentication and use advanced technology, such as secret keys and encryption, to verify a user's identity. The simplest example of strong authentication is a consumer's ATM card. This requires something the user has (their card), and something they know (their PIN). Most people wouldn't want their bank to allow access to their checking account with just one factor. Yet many organizations allow entrance to their valuable VPN, Citrix, and Outlook Web Access resources (often much more valuable than a single personal checking account) with only one factor—often a weak password. Strong authentication enables organizations to strengthen the protection of these vital resources.

While the decision to use strong authentication is clear cut, deciding on an approach is anything but. Today, there are hundreds of options, with each presenting its own specific advantages and tradeoffs. The following section offers a high level overview of the various alternatives available today.

## Overview of Authentication Options

Today, security teams can choose from a broad array of advanced authentication mechanisms. Following is a summary of these different approaches.

### Hardware

Generally, hardware-based authentication mechanisms come in several form factors: USB tokens, One-time Password keyfob models and credit-card shaped smart cards. While the variances of hardware-based authentication mechanisms are many, in general, these offerings can be grouped into one of three categories:

**One-time password (OTP).** These solutions have screens that display a randomly generated set of alphanumeric characters that constitute a password that can be used once. These random characters are sometimes changed on a regular basis, say, every 60 seconds, or they are changed after a user event, for example a user pressing a button on the token.

**Certificate-based.** Certificate-based hardware offerings use digital client certificates and public key infrastructure (PKI) for enabling user identification and access controls. Digital certificates are stored and transported on smart cards or USB tokens. Each certificate can only be used to authenticate one particular user because only that user has the corresponding and unique private key needed to complete the authentication process.

**Hybrid.** Finally, there are also hybrid tokens that provide a combination of OTP and certificate-based authentication within a single device.

*Today, organizations need strong authentication solutions that provide reliable security—and that are easy to install and deploy, simple to manage, and adaptable to changing needs.*

### Software

Today, there are many multi-factor authentication solutions that do not require hardware components. These software-based solutions fall into the following categories:

**OTP**. Software-based OTP solutions provide a means for securely delivering one-time use passwords to users, ensuring that if passwords are somehow disclosed, they will be rendered useless to a would-be attacker.

**SMS.** These solutions use information sent as an SMS message to the user as part of the login process. The process instituted can vary, but essentially, the approach is that a user looking to gain remote access submits a request for a password, which is then fulfilled via SMS to the user's authorized phone. This password is then used to gain account access.

**Certificate-based.** These software alternatives leverage PKI for the generation of digital certificates that form a means for authentication. As opposed to hardware alternatives, these certificates are delivered through software

## Hardware or Software Authentication? 5 Key Considerations

Today, organizations need strong authentication solutions that provide reliable security—and that are easy to install and deploy, simple to manage, and adaptable to changing needs. But how can decision makers ensure they're selecting the optimal technologies and approaches for their organization? The following section outlines the advantages of the options available, contrasting the relative advantages of hardware- and software-based offerings.

### Deployment

When it comes to the effort and time for deployment, software-based authentication mechanisms offer clear advantages. To start, no physical tokens need to be mailed, which eliminates shipment time, and the potential for routing delays and missed deliveries. In addition, some advanced authentication solutions feature "over the air" deployment to the user's mobile device, which both speeds and simplifies deployment efforts. These solutions can also equip end users with self-activation capabilities, which can offload the bulk of set up tasks from security administrators.

Finally, software approaches enable more deployment scenarios, expanding the reach of multi-

factor authentication to those usage scenarios in which distributing physical tokens would be too complex or costly. For example, banks could roll out strong authentication for online banking consumers, whereas distributing physical tokens would otherwise be too costly and would place too much responsibility on the consumer to be feasible. In the wake of a workplace evacuation or disaster, companies can immediately deploy and activate software-based authentication access to provide employees with access to critical network resources.

### Maintenance and Manageability

When it comes to ongoing management and maintenance, hardware-based alternatives can provide a benefit when combined with physical security devices and infrastructure. Many organizations have integrated the cards required for gaining access to buildings or for use as employee ID badges with the technologies used for online authentication, which can streamline up-front and ongoing administration.

On the other hand, software approaches can provide several key benefits in ongoing administration. Software alternatives completely eliminate the administrative burden of lost or broken tokens. In addition, when updates need to be made, whether to change user privileges, install security patches, or other tasks, many software solutions enable organizations to do these updates wirelessly, regardless of where the user or device is located, which can significantly streamline administration.

When looking at maintenance and management characteristics, it is also important to realize that, for many enterprises, the best approach may be to deploy both hardware and software for different groups and use cases. For those organizations, it is important to adopt authentication management solutions that can be used to centrally administer both hardware and software tokens.

### Total Cost of Ownership

By eliminating the need for hardware tokens, software-based alternatives present a range of savings, both initially and over the longer term. With no physical device to mail, organizations save in mailing costs, both for initial deployment and on an ongoing basis as devices need to be replaced. Software alternatives also eliminate the ongoing cost of purchasing tokens to replace those that have been lost or broken.

Finally, software presents advantages from a licensing standpoint. First, organizations only need to pay for the software license, while hardware solutions may entail both a software license and a fixed per-token subscription cost. This can result in significant cost savings, and can streamline pricing negotiations and procurement. Further, organizations can avoid the "time-bombs" some hardware token manufacturers use to force customers to replace tokens after a set amount of years.

*When looking at maintenance and management characteristics, it is also important to realize that, for many enterprises, the best approach may be to deploy both hardware and software for different groups and use cases.*

### End User Convenience

By eliminating the token, which the user has to protect and ensure it is available whenever access is needed, software can present significant advantages in convenience for end users. For example, they don't have to suffer lost productivity because they left a token at home before leaving for a trip.

Many software solutions leverage the users' mobile phone as an authentication device, which means users can work with a device they already use regularly and keep with them. Often these solutions make it easier to transfer credentials, so, for example if a user buys a new phone, it is relatively easy to pass the associated details over to the new device.

Software can also streamline the process of establishing connections by eliminating the physical steps required to insert tokens. Finally, software authentication mechanisms also afford security teams with the flexibility to turn to mobile devices or other software based authentication mechanisms as an interim replacement in the event a token is lost, damaged, or stolen.

### Security

In the end, authentication methods are employed because of security, so this is the most critical consideration in deciding on the most optimal authentication approach. When properly deployed, both hardware and software authentication alternatives can guard against a host of threats, including phishing and password theft. In addition, mobile phone based authentication mechanisms clear any trace of the secure login session from the mobile phone in order to eliminate the possibility of a thief extracting credentials from a lost or stolen phone.

While differences will vary depending on the specific solution and the manner in which it is employed, in general, having a purpose-built hardware device to deliver authentication capabilities affords the highest degree of security. These solutions inherently add another layer of defense, and another obstacle for would-be criminals.

Some of the more robust hardware tokens offer hardened manufacturing and certification with such standards as the Federal Information Protection Standard (FIPS) and Common Criteria standard. Finally, hardware tokens can be equipped with RFID-based location technologies, which can both serve as a deterrent and an invaluable way to track down lost or stolen devices.

Table 1. Hardware and Software Authentication: A Comparison

| | Hardware Advantages | Software Advantages |
|---|---|---|
| Deployment | | "Over-the-air" deployment speeds process. Broader deployment options. |
| Management and Maintenance | Combine with physical access mechanisms | Ability to wirelessly update user privileges and install patches reduces long term costs |
| Total Cost of Ownership | | Eliminates cost of purchasing, shipping, and replacing tokens |
| End User Convenience | | Easier to use, one less device to carry and guard |
| Security | Offers maximum security, including adherence with standards, RFID support | Guards against a range of threats |

## Conclusion

Strong user authentication is a critical mandate for many organizations today. In their efforts to meet this requirement, organizations can choose from a host of solutions. In making these decisions, criteria such as end user convenience, manageability, and, most importantly, security need to be evaluated. It is important to note that, for any given enterprise, choosing between hardware and software doesn't have to be an either/or decision. In fact, for many organizations, the right approach is often a mix of two or more authentication types, according to the needs of various usage scenarios and user groups.

## About SafeNet Authentication Solutions

SafeNet authentication solutions ensure easy and secure strong authentication for employees, partners, and customers and cover the entire spectrum of security needs, from remote access to advanced certificate-based applications. In addition, SafeNet offers the token management systems that streamline deployment, provisioning, and ongoing maintenance. SafeNet's token management systems support the company's entire range of hardware and software authentication solutions, which offers even further benefits in administrative efficiency—while enabling organizations to tailor authentication approaches to specific risk levels and use cases signing in a software-based solution.

*For many organizations, the right approach is often a mix of two or more authentication types, according to the needs of various usage scenarios and user groups.*

## OTP Authenticators

**eToken PASS**
The eToken PASS is an OTP token that offers two-factor strong authentication in detached mode. eToken PASS is available in both time and event-based versions.

**GOLD**
GOLD is an event-based OTP token that offers strong, two-factor authentication. It also supports challenge response functionality which offers an additional layer of security by generating the OTP only after users enter a PIN code on the token keypad.

## Certificate-Based Authenticators (PKI)

**eToken PRO**
The eToken Pro is a smartcard USB token that provides two-factor strong authentication, advanced security applications, digital signatures, and cost-effective password management.

eToken PRO Anywhere
The eToken Pro Anywhere is a clientless smartcard USB token that leaves zero footprint on end-user computers. It combines the strength of certificate-based, two-factor authentication with the plug-and-play simplicity and mobility of OTP.

**iKey 2032**
The iKey 2032 is a smartcard USB token that offers two-factor authentication, advanced security applications, and digital signatures.

**iKey 4000**
The iKey 4000 is a smartcard USB token that offers multi-factor authentication with optional match-on card biometric functionality.

**eToken PRO Smartcard**
The eToken Pro is a credit card form factor authenticator that supports password management, digital signatures, and advanced security applications.

**SafeNet Smartcard 400**
The SafeNet Smartcard 400 is a credit card form factor authenticator that supports certificate-based, multi-factor authentication and advanced security applications.

## Hybrid Authenticators

**eToken NG-OTP**
The eToken NG-OTP is a hybrid USB token that supports both OTP and certificate-based authentication.

**eToken FLASH**
The eToken NG-FLASH is a certificate-based, strong authentication USB token with on-board encrypted storage. eToken NG-FLASH is available in sizes ranging from 1GB to 16 GB.

## Software Authenticators

**MobilePASS**
MobilePASS is a software-based OTP authenticator that combines the security of two-factor strong authentication with the convenience of one-time passwords generated on Windows desktops and a range of mobile devices, including iPhone, BlackBerry, and Windows Mobile platforms. For additional flexibility, it also supports SMS delivery to mobile devices.

**eToken Virtual**
eToken Virtual is a certificate-based, two-factor authentication solution that provides full PKI functionality, including secure remote access, network access, and digital signing in a software-based solution.

To learn more about SafeNet Authentication Solutions, visit www.safenet-inc.com/authentication

**Contact Us:** For all office locations and contact information, please visit **www.safenet-inc.com**
**Follow Us:** www.safenet-inc.com/connected