Strong Authentication Implementation Guide
Introduction

Secure and convenient strong authentication to protect identities and access to IT infrastructures is a key factor in the future of enterprise security. In the banking sector alone, Gemalto has contributed to large scale authentication rollouts for more than 3,000 financial institutions worldwide, with 50 million authentication devices delivered directly to our clients’ customers.

Through our knowledge and experience as the global leader in digital security, we have identified key steps to successfully implement strong authentication in your organization. The steps are presented in this guide.
IT security risks are changing and increasing in complexity. Are you keeping pace?

Recently the news has been filled with story upon story of security leaks and breaches.

- Dubbed the Internet’s worst nightmare, the Heartbleed bug exposed a vulnerability in OpenSSL that provided hackers the opportunity to steal passwords, credit card data or Social Security numbers from two-thirds of all websites.

- The most successful one-day cyber attack against a government was the Columbian Independence Day Attack on July 20th, 2013. Web application and network DDoS attacks managed to completely shut down most government websites for the entire day.

- Retailers were hit hard in 2013, with Target and Neiman Marcus taking the hardest hits with 110M and 1.1M customers affected respectively.

- Healthcare suffered the highest number of attacks by any industry in 2013, over taking the business sector for the first time in almost 10 years. Healthcare had 267 breaches—43% of all attacks.

- Intensive and protracted DDoS attacks staged in waves were the cause of the longest and the largest cyber attack in history. The target? US financial institutions.

- Social network sites Twitter, Instagram, Snapchat, Skype, Facebook, Yahoo, LinkedIn, and Evernote, have all been hacked in recent years, amounting to millions of stolen user accounts.
The password problem

Humans aren’t wired to remember passwords, hence why we see laughably weak passwords such as “123456” in use today. If we are to progress towards more secure and convenient authentication solutions, we have to start thinking beyond passwords. Multi-factor solutions that operate independent of passwords, are the future.

The reason for the increase is that the threatscape has changed dramatically in recent years. Hackers are increasingly able to penetrate endpoints and download Trojans, keyloggers and other malware onto endpoint PCs or laptops to steal login passwords. Here are some of the reasons why they are winning the endpoint security fight:

> Hackers change malware so frequently that signature-based endpoint defenses like anti-virus software can’t stop them, so basically every day is zero day.

> Command and control toolkits like ZeuS and SpyEye make it easier for hackers to manage zombie botnets and mount attacks.

> Hackers target high-value companies with many combined attacks over time, so called Advanced Persistent Threat [APT] attacks.

In looking at the individual cases, over-reliance on password authentication is a common problem that enables cyber criminals to penetrate networks. If anyone who has access to your network is attacked, hackers can steal passwords and get a toehold in an IT infrastructure. From there, they expand to more valuable targets, such as system administrators, eventually creating their own system management accounts. If password-only authentication is allowed, even for system administrators, hackers can create new accounts or access and copy any file they choose.

Understanding the threat should raise real questions about your security strategy:

> Is your security dependent on passwords?

> Do you need stronger security for network access?

> Are you relying on signature-based anti-virus software, leaving you vulnerable?

> Does your security depend on every employee, and perhaps their family members, never falling for a well-crafted phishing attack?
Strong, or multi-factor authentication is defined as authentication that uses two or more different forms of identity verification. An example of true multi-factor authentication could be where a user is required to insert his or her smart card (something they have) into a reader, and then must enter a PIN or passphrase (something they know) in order to unlock their credentials and access a secure network. If they have also have to place their fingertip (something they are) on a biometric fingerprint reader, this would add a third factor of verification. Each level of identity verification adds a further layer of protection.

Implementing strong authentication provides a simple and cost effective way to:

- Mitigate the threat of impersonation for sensitive accounts
- Enable secure remote access for mobile workers
- Increase convenience by removing the need for complex and costly password policies
- Lower password maintenance costs
- Build the foundation of a comprehensive Identity Management Roadmap.

Strong authentication technology significantly strengthens the fabric of the layered security because it adds "something you have" to the authentication process. A hacker who steals passwords or attempts to create his own admin accounts will be blocked by the strong authentication device associated to the identity he wants to use. When well-engineered, the second factor of authentication can be virtually impossible to duplicate.
Many leading information technology organizations recommend strong authentication solutions as an element of a strong IT infrastructure. For example, Microsoft’s Core Infrastructure Optimization (IO) model is a structured process that helps organizations better understand and strive for a more secure, well-managed, and dynamic core infrastructure that will help reduce overall IT costs, make better use of IT resources, and make IT a strategic asset for the business.

As part of its Identity & Security Management discussion, Microsoft says, “How much does it cost every time a user calls a help desk to ask for his or her password to be reset? This issue has plagued the IT world for decades, and the most common solution leads to more security breaches than any other single security issue.”

Among other things, this model defines strong authentication, PKI certificates and smart cards as important attributes of a well-managed identity infrastructure using Microsoft’s Forefront Identity Manager. Specifically, it recommends credential management that:

- Enables users to reset their own passwords through both the Windows logon and the Forefront Identity Manager password-reset portal, which lowers help desk costs.

- Provides effective implementation of strong authentication with integrated smart card and certificate management.

- Increases access security beyond username and password solutions.

- Simplifies certificate and smartcard management using Forefront Identity Manager.

- Enhances remote access security through certificates with Network Access Protection.

- Includes stronger authentication through certificates for administrative access and management.

- Controls help desk costs by enabling end users to manage certain parts of their own identities.

- Improves security and compliance with minimal errors, while managing multiple identities and passwords

A second organization that recommends strong authentication and PKI certificate-based smart cards for higher levels of trust in identities is the U.S. National Institute of Standards and Technology (NIST).

In response to Homeland Security Presidential Directive 12 (HSPD -12), which called for one very secure identity management and security credential across the entire U.S. federal government, NIST has worked out a framework for strong authentication and defined different levels of identity assurance. This body of work underlies the U.S. federal government’s own secure identity credential, the Personal Identity Verification (PIV) card, issued to all federal employees and subcontractors.

The standard defines four Assurance Levels ranging in confidence level from low to very high. The level of assurance is measured by the strength and rigor of the identity proofing process, the credential’s strength and the management processes the service provider applies to it. PKI certificate-based smart cards are Level 3 [high] and the same level as the PIV cards and the Department of Defense’s equivalent, the Common Access Card (CAC).

SUPPORTING DOCUMENTS

- Special Publication 800-63, Electronic Authentication Guideline

- Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors

- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
Consider your users’ needs

When evaluating the best way to move forward with implementing strong authentication, start by analyzing who you need to protect and what activities need to be protected. For example, not everyone in a company will need the same level of access to critical business information. For a remote salesperson, access to their email and CRM may be all they need. For an executive traveling, the access requirements are much broader, and the information being accessed will most likely have a higher degree of sensitivity. This is where a layered approach provides the right protection for the right business need.

Enabling a mobile workforce to gain secure access to corporate resources can provide a competitive advantage allowing a quicker response to customer questions or sales proposals, or improve employee productivity and customer service, as examples. But while mobility can increase productivity, it also introduces a significant security risk. With numerous potential entry points into the network, the new challenge for IT security professionals is balancing security with convenience.

Today, there are several tools available to IT security professionals to secure remote connectivity. VPN, access control gateways and intrusion prevention systems all play a role in ensuring only the right people have access to corporate data. But with the sophistication of these access control systems, in most cases the primary identity verification method is still a basic username and password. This is similar to purchasing a Ferrari and installing skeleton key locks on the doors. The two simply do not line up.

Even with the sophistication of heuristics, access control list, data flow analysis, etc., an intruder can easily access the network undetected if they are logging in using legitimate credentials. To mitigate this, companies have implemented increasingly complex password schemes and forced users to change their passwords every 30-90 days. While this makes it more difficult to guess a user’s password, the result has been more user lockouts and password resets through the help desk—with every call costing the company time and money. Implementing strong authentication makes life easier for employees, by removing the requirement to remember many different and frequently changing complex passwords.

Another distinct class of users is C-level executives and senior managers involved in sensitive topics like mergers and acquisitions, corporate earnings forecasts and not-yet-disclosed investor releases. Requirements for this group can include:

- Secure email encryption/decryption.
- Digital signature of electronic documents.
- Strong authentication for hard disk encryption.
- Multi-factor desktop and remote access.

Similarly, system administrators not only have unique needs, but this group should be among the first of individuals required to use strong authentication in any organization. Hackers strive to work their way through an organization and get to a system administrator’s account, and then set themselves up with their own admin account. At that point they can do virtually anything they want within the system or network.

To stop this from happening, require strong authentication for all of your system admins before they can have access to make certain types of changes, such as creating new system admin accounts. There are many other examples, but the key is to look at all of the use cases in your organization. This will prepare you to look for technology solutions that can address all of the different requirements.
As you plan a strong authentication implementation, you must examine how it can fit into your current IT and security infrastructure. Fortunately, Gemalto has partnered with leading IT vendors such as Microsoft, Citrix, Adobe and many others to make this step easy.

On the backend, Gemalto makes it simple to install its IDConfirm Authentication Server. It can be installed on an existing infrastructure in less than 10 minutes for initial configuration. The server works with leading identity store providers such as Microsoft Active Directory and can quickly sync between IDConfirm and existing user information for OTP seed provisioning, for example.

An alternative for the backend is to use hosted services, which simplifies and speeds up the implementation and lowers up-front capital costs. Gemalto offers IDConfirm as a hosted service, for example, and it is still easily integrated with the existing infrastructure.

You may have deployed other security devices, so a requirement may be for these legacy devices to co-exist during a transition period. If you are in the process of phasing out one vendor and moving to Gemalto, the Gemalto OTP solution can co-exist with your other authentication provider.

You need to carefully examine the applications you want to use with your strong authentication implementation. Many common programs, such as Microsoft Windows, Microsoft Office, Adobe Reader and Citrix Presentation Manager, natively support Gemalto strong authentication. Gemalto also provides an open API to enable easy integration with existing applications and IDConfirm.
Not all users are created equal. As mentioned before, there are different roles within each company requiring different access privileges. Simply put, implementing strong authentication should not be one size fits all. Gemalto has a full portfolio of strong authentication options so you can implement the right technology to address each specific business need. Solutions range from one-time password (OTP) technology to full certificate-based identity solution enabling data encryption and digital signature.

TECHNOLOGY CONSIDERATIONS

As you examine technology options, consider these as requirements:

- Offer a wide portfolio of strong authentication solutions, from OTP to PKI certificate-based. This allows you to choose the level of protection that best fits the needs of your organization.
- Offer a variety of different form factors, including ID credentials, unconnected OTP devices, dual unconnected/connected USB tokens and mobile solutions.
- Support open industry standards when available (e.g., OATH for OTP).
- Offer a server platform to facilitate implementation.
- Provide a versatile authentication platform that supports a full range of devices and technologies.
- Capability to set and enforce risk-based authentication policies that raise the level of security required for certain types of higher risk logins and deny or scale back access privileges.
- Availability of cloud-based outsourced device provisioning.
- Solutions for securing cloud computing and mobile workforces.
One-time password (OTP) is a good first step in securing your network, especially when granting access to remote users. OTP provides an additional layer of security to username and password. The user simply enters a username and the numeric code provided by the OTP device. The authentication server validates the code, and access is granted to appropriate network resources. This increases the security of the login process by ensuring the person accessing the network is in possession of two factors of identity verification. In this case, the OTP device and a username and potentially a password. This means that someone cannot simply find a password written down or obtain credentials through social engineering. They actually need to have the OTP device and the right code in conjunction with the user’s other information.

There are two other important benefits to IT teams that implement OTP-based security:

- OTP solves VPN headaches by eliminating the need for a VPN client, replacing it with OTP Windows logon
- It allows employees to use their mobile phones—something they already have—for OTP.

Mobile OTP also enables organizations to have full ownership of their key management through self-provisioning using recognized methods such as the IETF reference standards for Open Authentication Organization (OATH) key provisioning. This means that there are no dependencies on the vendor maintaining the confidentiality of the keying material. The phone also enables PIN validation by the user during the OTP authentication process, further increasing security and identity verification.
Step 7 | Move up to PKI certificate-based identities

While OTP authentication for network access is a significant step-up from user name and password, certificate-based authentication raises the bar even further.

As discussed earlier, leading reference frameworks such as Microsoft’s Core IO and the federal government’s authentication guidelines and FIPS 201 standard, recommend credentials and processes based on PKI certificates and smart cards for high levels of security and identity assurance.

With a solid identity foundation that includes consolidated ID repository, good data sources and a mature ID provisioning system, deploying certificate-based authentication is easy and can be done at a minimal cost.

Gemalto’s Protiva smart card-based solutions leverage public key infrastructure (PKI) to provide certificate-based strong authentication. This ensures two-factors of authentication by leveraging the smart card product (card or token) for something you have, combined with a user selected PIN for something you know to provide two factors of authentication. With proper security controls in place to verify the identity of the user before smart card issuance and certificate provisioning, you can be assured that only the legitimate user is the one accessing the corporate network and sensitive data. Once a certificate-based identity solution has been deployed; there are several additional security features that can be added. Some of the notable features include:

- File encryption – The problem of securing the Data-at-Rest (DAR) has been resolved, and hard drive encryption is the solution. While OTP increases network access security, it brings little value to hard drive encryption; however, certificate-based smart card security can be used together with disk encryption systems to provide multi-factor authentication for decrypting sensitive files or hard drives.

- Email encryption – Ensure the security of sensitive information through email. Leveraging the cryptographic process within the smart card deployment, email is encrypted and can only be decrypted by the intended recipient – keeping your email safe from unwanted eyes.

- Digital signature – Using the Internet for business processes is cheaper and faster, but these savings can be negated by having to rely on “wet” signatures for validation and approval. Digital Signatures created using Protiva smart card devices with PKI can securely authenticate virtual documents saving both time and money.

- Mutual authentication – As hosted applications become more prevalent, there is a need for stronger controls both from the system to authenticate the user and also the user being able to authenticate into the system. This provides an additional layer of security to ensure information exchanged online is secure, and the user is interacting only with the legitimate application.

Implementing PKI certificate-based smart cards brings your IT infrastructure in line with the high levels of e-authentication security recommended by security specialists at Microsoft and NIST.

RISK APPROPRIATE AUTHENTICATION

- Not all users are created equal. Each user accessing the network has a set of requirements based on job function and access needs. When implementing strong security controls, user needs and the ability of IT security to support these needs will require a flexible security solution to meet these varied user profiles.
There are three options when deploying a certificate-based identity solution: .NET, minidriver enabled (MD), or PIV. Each solution provides a high level of assurance of the identity of the user attempting to gain logical access to the network. These smart card-based products can be combined with proximity technology to also provide for physical access, and with security printing processes, can serve as visual identity as well.

.NET and MD smart cards leverage the built-in card management capabilities in Microsoft Server and Windows OS. This deployment requires no additional middleware for card management. Fully contained within Microsoft Forefront Identity Manager (FIM) a .NET or MD certificate-based authentication solution is virtually plug and play. .NET & MD are also compatible with MAC OS and Linux environments. Adding biometric functionality adds a further level of security with the addition of fingerprint match-on-card user verification. This functionality is supported by Windows Biometric Framework.

Additionally, MD smart cards exists with a certification according to US regulations (FIPS 140-2 Level 3) or European regulations (CC EAL5+ / PP SSCD). MD smart cards can also be manufactured as dual interface and are compatible with the NFC interface present on many smartphones and tablets.

As reflected by the FIPS 201 certification, PIV smart cards fully conform to the solution selected by the U.S. Department of Defense. This is the identity card base for both the Common Access Card (CAC) used by millions of military personnel and the Personal Identity Verification (PIV) identity credential used by non-military federal agencies.
Step 9

To get started quickly, use cloud-based services and channel partners

A fast way to get started is to use a technology provider that offers a combination of supporting security partner specialists and Web-based services. Gemalto has strong security channel partners worldwide to help you plan and implement your strong authentication solutions.

If you think Web services can help simplify and accelerate deployment in your large enterprise, consider requiring these of your technology provider:

> **Complete fulfillment service**

Why maintain a stock of OTP tokens? Gemalto can provide complete OTP fulfillment including order handling, packaging, shipping, tracking and provisioning the OTP hardware device (token or display card).

For the mobile OTP app, Gemalto provides a portal for redirection to the appropriate app store based upon the user’s smart phone device (i.e., redirected to Apple app store for iPhone app download).

> **No batch fulfillment requirement**

Gemalto will ship an individual hardware OTP device to an individual end user or provides the option to ship in batches to a central distribution point.

> **Web store option**

Gemalto can create a custom web store for your users to order their OTP device and provide shipping information. For cost allocation, each device or batches of devices could be purchased through the web store attributing the cost to the specific group or cost center associated with the user.

> **Automated seeding process**

By syncing with an existing identity store, IDConfirm simply links an OTP seed with the user account. This allows the user to self-activate once they have received their OTP device or downloaded the mobile OTP app.
Mobile phones have become ubiquitous, and smartphones continue to gain significant momentum especially in developed countries. This has introduced an interesting option for OTP technology – leverage the mobile device as an OTP token.

There are two ways that this can take place. The first is to use the short message service (SMS) capability within every mobile device. The user requests an OTP when logging in to a specific resource and receives one back from the network.

The second option is to have an app that can be used on a smartphone. When a user is required to enter an OTP for strong authentication, he or she simply launches the app which generates an OTP eliminating the need for an additional hardware device. Gemalto also has one-touch user authentication, which once the user receives the OTP from the app, they simply push send passcode. No need to physically enter the OTP.

Another option is to use a smart card ID with a mobile device. The mobile must be connected to a special reader device with either a cable, as a sleeve around the mobile device, or via Bluetooth wireless technologies. The NFC interface, when available on the mobile, can also be used with dual interface cards.

The future of mobile security: The Secure Element

As the mobile industry advances and standards mature, more security options are becoming available to store digital ID credentials directly in a hardware-based «Secure Element» that is part of a smartphone or mobile tablet architecture. The Secure Element is based on smart card technology such as a SIM/UICC card, a MicroSD card or an embedded Secure Element chipset.

In all these cases, the Secure Element is the key security factor that generates and stores cryptographic secrets and performs the associated algorithms needed for strong authentication and other digital security services.
Learn more
When the time is right, consider contacting Gemalto. Our Protiva family offers a full spectrum of strong authentication solutions, from OTP to PKI credentials in cards or tokens. Our Protiva IDConfirm server can fit simply into your infrastructure, and Gemalto gives you many options for deployment, from enabling your in-house management to cloud-based services for hosting of provisioning on-boarding.

About Gemalto

As the global leader in digital security, Gemalto solutions enable some of the world’s best known organizations to protect user identities and IT resources without compromising convenience or efficiency. We develop secure embedded software and secure products which we design and personalize. Our platforms and services manage these secure products, the confidential data they contain and the trusted end-user services they enable. Our innovations enable our clients to offer trusted and convenient digital services to billions of individuals. Gemalto thrives with the growing number of people using its solutions to interact with the digital and wireless world.

Visit gemalto.com/identity
Follow our blog at: blog.gemalto.com