WHITE PAPER

Authentication Best Practices:

Put Control Where It Belongs

A significant number of high profile security breaches have occurred recently, bringing the organizations affected to the front pages of the business press. These events have had a negative impact on the public image of these companies, and may also have a harmful effect on their business. These incidents have caused the CIOs of many companies to re-evaluate their info-security strategy in general, while also placing specific focus on their user authentication and transaction security requirements.

These breaches are a reminder that any company may become the target of an attack for its customer, financial, and other confidential data, as well as its intellectual property assets. In response to these threats, a comprehensive, layered approach to security and authentication is essential to protecting an organization's vital and sensitive information and systems. This paper suggests a set of best practices for user authentication.

Benefits of a Fully Trusted Authentication Environment:

- Enables customers to create their own token data, and retain control of security data and policies
- Offers additional layers of protection through encryption of token data, and the ability to store and manage keys in hardware
- Addresses varying user risk levels and user requirements with authentication choice such as: certificate-based authentication, OTP, mobile authentication, and secure access to SaaS applications
- Improved management and visibility, with centralized and simplified administration, deployment, and manageability
- Industry proven, using standards-based algorithms; no proprietary technology

The Gatekeeper for a Robust Info-Security Solution

Security solutions need to be managed in a layered approach that combines encryption, access policies, key management, content security, and, of course, authentication, just like any other component in the datacenter. These layers need to be integrated into a flexible framework that allows the organization to adapt to the risks it faces. Each of these items can be broken down further in order to develop best practices when evaluating, deploying, and maintaining such items within the information protection lifecycle (ILP).

An authentication solution that ensures the identities of users and computing devices that access the non-public areas of an organization's network is the first step in building a secure and robust information protection system. Lack of proper authentication mechanisms can cause a chain effect that will hamper an organization's ability to protect information throughout its lifecycle.

Recent breaches have highlighted vulnerabilities in the deployment of authentication solutions. Deploying an authentication solution in a robust way will ensure that the identities of users in the system are validated upon entry and thus create the first layer in a multi-layered info-security architecture.

User Authentication Best Practices

In the aftermath of recent breaches, organizations are closely examining their authentication solutions. To best understand the risks they are facing, organizations are advised to analyze a range of factors relating to IT policy, regulations and compliance, employee behavior, and data storage. Once organizations have a risk model in place and are more aware of their vulnerabilities, they are in a better position to minimize the risk of a breach, and to develop an authentication strategy suited to their needs. This strategy needs to be defined according to their business and their users, who will be required to authenticate for access to the system. Taking these factors into consideration, the CIO can define a layered approach to authentication that includes the core authentication system, the lifecycle of authentication components, and complementary solutions.

As companies re-evaluate their strategies to mitigate their info-security risks, they should look closely at best practice recommendations as follows:

Core Authentication System

Match Your Authentication Solution to Your Business, Users, and Risk

A flexible approach that enables an organization to implement different authentication methods based on different risk levels may ensure a robust system that can be efficiently and cost-effectively deployed.

Technologies for multi-factor authentication include:

- **One-time Passwords (OTP):** OTP technology is based on a shared secret or seed that is stored on the authentication device and the authentication backend. This method ensures authentication by generating a one-time passcode based on the token's secret.
- **Certificate-based Authentication (CBA):** This method ensures authentication using a public and private encryption key that is unique to the authentication device and the person who possesses it. CBA tokens can also be used to digitally sign transactions and to ensure non-repudiation.
- **Context-based Authentication:** Context-based authentication uses contextual information to ascertain whether a user's identity is authentic or not, and is recommended as a complement to other strong authentication technologies.

In order to develop a robust authentication solution, organizations should consider their business, users, and risk, and select a solution that provides them with the flexibility to adapt as needed. For example, if organizations are interested in implementing additional security solutions that rely on PKI technology, such as full-disk encryption, network logon, and digital signatures, or are thinking about adding such solutions in the future, they should consider CBA, as it enables these applications.

Strengthen OTP Solutions with a User Shared Secret

For OTP authentication, an additional layer of security can be implemented by adding a PIN of 4 to 8 digits to the one-time password that is created by the token. The OTP PIN is "something only you know" – a fundamental precept for two-factor authentication. This ensures that even if the token-based authentication mechanism is breached, the hacker still needs to know the user's PIN in order to access the system.

Prefer Solutions that Adhere to Standards-based Security and Certifications

Products that are built upon standards-based crypto-algorithms and authentication protocols are preferred. Unlike proprietary algorithms, standards-based algorithms have gone through public scrutiny by industry and security experts that reduces the chance of any inherent weaknesses or vulnerabilities. Moreover, they enjoy broad industry support.

The use of products that have undergone validation by an accredited third party, such as FIPS (Federal Information Processing Standard) or Common Criteria certification, ensures that they conform to the industry standard.

Consider All Access Points

Organizations need to ensure that access to all sensitive information is authenticated, whether the information resides on premise or in the cloud. Organizations should implement the same security mechanisms for cloud resources as they would for remote access to the corporate network.

In addition, organizations should deploy security mechanisms to ensure that users accessing network resources from their mobile consumer devices (e.g., tablets, smart phones) are securely authenticated.

Implement Effective Password Management Policies

In all instances where passwords are required, such as to ensure the authenticity of the user or when setting passwords for CBA tokens, Gemalto recommends the following password management practices:

- Organizations should not allow the use of default passwords.
- Organizations should enforce passwords that are based on a mix of uppercase and lowercase letters, and numbers.
- Password length should be at least 8 characters.
- Organizations should not allow passwords that are the same as the user's name.
- Organizations should enforce password replacement on a regular basis. The length of time between password replacements should be based on risk profile but should be done at least once every three months.

Robust OTP Authentication Deployment

Complement Authentication Solution with Robust Key Management

One-Time Password authentication systems are based on a shared secret, usually referred to as the OTP seed (or token seed value). This seed is used to generate the one-time passcode. The OTP seed is stored on both the token and the authentication management system.

The effectiveness of the OTP authentication mechanism relies on the secrecy of the OTP seed, as well as the cryptographic strength of the algorithm employed to generate the one-time password. If one of these elements is compromised, the strength of the entire authentication solution is weakened.

In most cases, the authentication system vendor programs the seeds into the token and provides the token information to the customer. When the token is assigned to a user, the link is established between the user and the authenticator. These assigned token seeds, associated with user authentication profiles, are used by the authentication manager to control user access to information.

Key management helps to prevent insider theft and malware by storing the security data in an encrypted file system or database. Since all authentication systems are comprised of some type of secret information, protection of the secret data is paramount. Therefore, it is recommended to encrypt the database, for example, of an OTP authentication system that stores the tokens' seeds, and the information that links seeds to tokens and users in an encrypted database. Managing the encryption keys that unlock this data has become critical to a comprehensive security approach. To achieve robust key management, customers can store encryption keys in a hardware security module (HSM).

Control Security Data On-Premise

Organizations that perceive their risk profile as high may create another layer of security by programming the token seeds in their datacenter. Field-programmable tokens give organizations the ability to generate the token security data and securely program it on their premise. For organizations perceived to be particularly at risk, relying on the security of a vendor is another variable not under their control, regardless of the security measures taken by the vendor. This recommendation is mostly suited to sectors where security concerns are much more salient, such as financial services, healthcare, and government.

Complementary Solutions

Use Pre-boot Authentication to Protect a Mobile Workforce and Portable Devices

For critical components of the system, organizations should examine the need for pre-boot authentication. This ensures that only selected employees can boot the system and perform administrator-based operations.

For users that store sensitive information on mobile devices and laptops, full disk encryption with pre-boot authentication (certificate-based) helps to ensure that the data on a lost or stolen device will not be exposed.

Develop Auditing and Forensic Capabilities

Audit trails and forensics can facilitate early detection if an organization's system has been breached. Audit trails are effective since they provide information about successful and unsuccessful authentication attempts to the system. The most obvious indicator of an attack is a sharp increase in the number of failed login attempts and account lockout, but this is usually the work of a clumsy, unsophisticated hacker. Generally, lockout policies limit this type of attack. More skilled hackers will patiently try a very low-volume series of login attempts or will resort to social engineering methods such as calling the help desk to request a reset of the PIN/password. Without effective audit tools, this type of attack might go unnoticed.

Context-based Authentication Complements a Layered Approach

Context-based authentication uses contextual information to ascertain whether a user's identity is authentic or not. Based on risk profiles, organizations may limit access to specific systems or content items based on a user's criteria, including whether the user is authenticating from the local or remote network, whether the user is accessing information from a corporate computer, or whether the access time appears reasonable (i.e. office hours for that user's country location based on their computer IP address). Since much of the information used by context-based information is publicly available and therefore easily accessible to hackers, it is recommended to use this method to complement other stronger authentication methods or as a first level of authentication in a multi-layered approach.

Versatile Authentication for a Comprehensive Security Framework

Gemalto, recognizing the growing complexity of maintaining security controls in this diverse landscape, offers organizations integrated product suites for ensuring authorized access and managing all multi-factor authentication operations for employees who need to securely access on-premise and cloud-based applications, and for customers and partners who do business online.

Gemalto's award-winning solutions provide an extensible, comprehensive foundation for securing an organization's strong authentication and transaction verification needs.

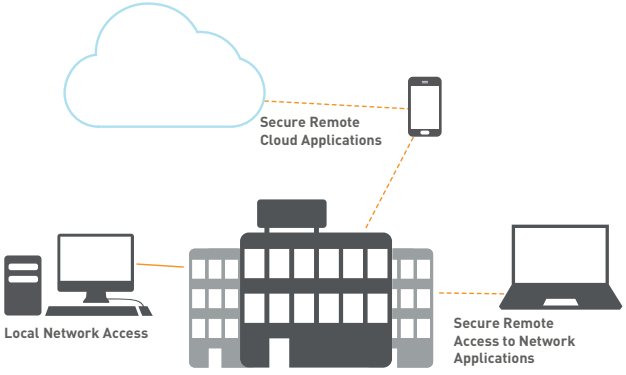
Gemalto's Fully Trusted Authentication Environment

Gemalto is the first to offer an authentication framework that provides enterprises with superior security, flexibility, and control over their authentication environment. The framework includes:

- **Field-programmable tokens:** Allows customers to generate the token security data and program on-premises. Gemalto is one of the only vendors to enable on-site token programming for OTP tokens. CBA tokens are automatically reprogrammable.
- **Offers additional layers of protection:** Encrypt token data and store/manage keys with an HSM
- **Improves management and visibility:** Centralized and simplified administration, deployment, and manageability
- **Industry proven:** Standards-based algorithms; no proprietary technology

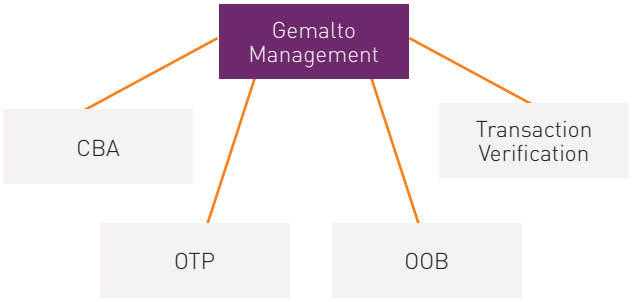
Gemalto's Family of Authentication Solutions for Secure Remote, Local, and Cloud Access

Gemalto's enterprise solutions enable organizations to meet security needs and plan for contingencies without having to change their underlying infrastructure. Offering flexible management platforms, the broadest range of strong authentication methodologies and form factors, and transaction verification capabilities, as well as identity federation and federated login, Gemalto solutions create a future-ready security foundation that allows organizations to adopt a modular, forward-looking identity management strategy, ensuring that their security needs are met as new threats, devices, and user needs evolve.



Gemalto authentication solutions are all managed by a single authentication platform, which enables:

- Secure remote access for employees and partners
- Transaction security for online banking
- Embedded cloud support for secure access to SaaS applications
- Secure access to corporate resources from mobile devices
- A single authentication server for centralized and simplified management
- A fully trusted authentication environment for customer control over their own data



To learn more about Gemalto's complete portfolio of authentication solutions, visit our website at www.safenet-inc.com/authentication.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

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

GEMALTO.COM

gemalto
security to be free