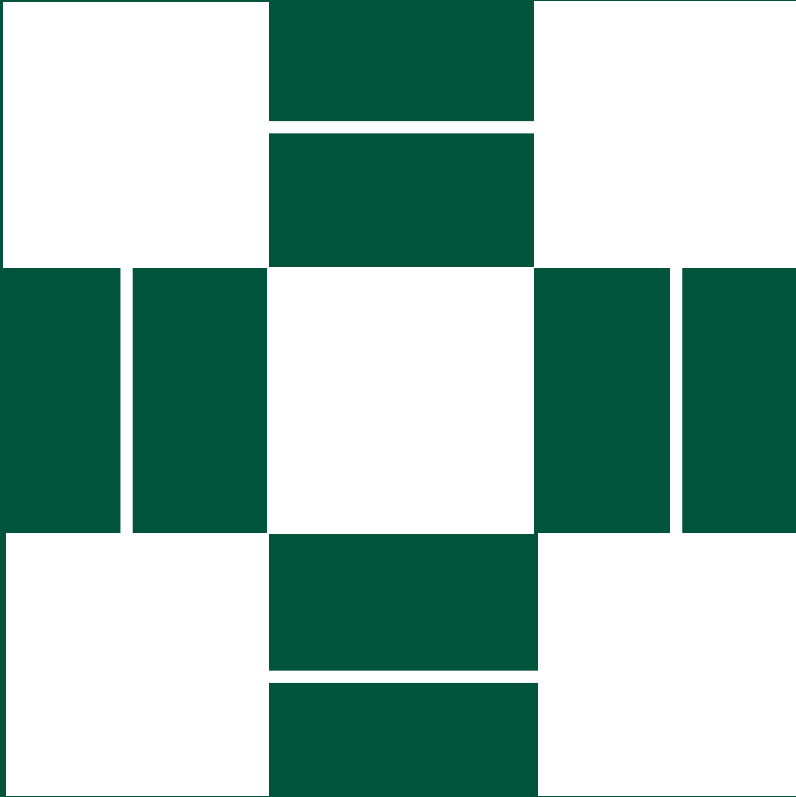


Strong Authentication



**MBA Residential Technology
Steering Committee (ResTech)**

Information Security Subgroup

ResTech Security

Strong Authentication White Paper

Strong Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. This authentication process can be confirmed through the use of one or combination of the following factors: 1) something you know (password), 2) something you have (token, certificate, etc.), and/or 3) something you are (biometrics – finger print, retina scan, etc.).

Authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. The weakness in this system for transactions that are significant (such as the exchange of money or Personally Identifiable Information - PII) is that passwords can often be stolen, accidentally revealed, or forgotten. This weakness has created the need for a more stringent requirement for what is often referred to as “strong authentication”. This enhancement affects how the password factor (something you know) and/or the use of other factors are constructed and used to identify an individual.

The use of multiple factors (2 or 3 factors in combination) is the preferred method of strong authentication. The banking ATM card is a good example of two factor authentication--1) the card - something you have, and 2) the Personal Identification Number (PIN)--something you know. Biometrics is the other authentication factor; however, it has some unique privacy and technology issues to overcome before it becomes more broadly accepted.

A hybrid method that has gained acceptance as a form of strong authentication is the use of a password in combination with other PINs/passwords (secret questions, selection of a favorite image, etc.). This method is not as strong as the use of multiple factors; however, its ease of implementation has gained adoption in many online financial/PII transaction environments.

Addressing Strong Authentication

Because it Makes Sound Business Sense

For a moment forget about regulation, audit and other reasons for implementing strong authentication and ask yourself this question: Why do we implement any security measure? The answer is because it is in the best interest of our customers and our company. Financial Institutions, be they chartered and regulated or not, have been entrusted with sensitive information by their customers. Trust has been placed in these organizations to protect this information and use it only for the purposes for which it was intended. As a financial organization, you must evaluate your current security strategy and compare that to the changing threat landscape. What was acceptable two years ago

may not apply today. As the Internet evolves, as companies provide more information and services online, and as attackers change their strategies, companies must keep up.

Legislatures have made it a priority

In October of 2005, the Federal Financial Institutions Examination Council (FFIEC) published an update to their August 2001 guidance for *Authentication in Internet Banking Environment*. This update was released in response to the considerable technical and legal changes and challenges since the original document was published. The guidance did not focus on a particular technology, but instead addressed the need for risk assessments, customer awareness programs, and risk mitigation strategies by the organizations.

What can be done?

Beyond Passwords

Passwords-- “something you know”--are considered the least secure authentication factor. The threat scenarios against passwords are many and don’t require sophisticated attacks. User IDs and passwords can easily be shared or intercepted. Surveys estimate over 40 percent of people choose one single password and another 45 percent use a small handful of passwords for most systems. Given these facts about passwords, what is the probability that the same password is used for both business and personal applications? If so, what control or policies does your business have over other systems? How difficult is it to control the integrity of a password?

Regulatory guidance and best practices recommend multiple factors or layered authentication for non-public personal information and financial transactions. A single factor password or PIN is vulnerable to a number of threats and the impact can be severe if unauthorized information disclosure were to occur. Businesses spend a great deal of money to protect their networks; unfortunately easily guessable passwords can be the Achilles heel of a security program.

Solution Factors

There are a number of strong authentication solutions available in the market. Depending on the business goals an organization is trying to achieve, the requirements for the solutions may vary from organization to organization. Basic requirements include, but are not limited to: cost, user online behavior, user preference for and acceptance of the technology, user experience, solution offerings in functionalities, system integration, vendor support, and the soundness of the solution providers.

There is no one model or methodology that can be used as guidance for all businesses. The unfortunate reality is that there may be more than one authentication process for your business. Do customers require a logical ID for a one time event (closing) or do they need recurring access to services (servicing)? What is the exposure with your business partners, financial transactions or personal information? Obviously, no solution is practical if it is inconvenient to your customers, partners or employees.

While the specific risks associated with each application should be evaluated separately, authentication methods can be shared between services. The ability to leverage authentication practices between services leads to efficiencies and reduction of processes. Services that have similar risk profiles can utilize a common authentication method. Strong (high assurance) authenticated credentials can be used by lower risk services.

Solution Options

Each of the solution providers offers their strong authentication by providing different factor(s) for authentications. These factors are usually based on “something you have”, “something you know”, or “something you are” principles. Each of the solutions/products offers strengths in some areas and trade-offs in other areas or features.

Shared Secrets and Images

Shared secrets are something a person knows, and are selected by the user during the initial contact. Both the user and the authenticating system (web site) have knowledge of the secret. Passwords, PINs, questions or pass-phrases are examples of shared secrets. Another method is user-selected images that must be identified or selected from a pool of images. Single factor shared secret is not considered strong authentication.

Cookies

Cookies are something a person has and are loaded onto a user browser by the web server. Cookies contain authenticating (user ID and password), tracking (shopping cart), or specific information. End users have no interaction with cookies. Authentication Cookies should be encrypted and coupled with another authentication factor such as a shared secret.

Tokens

Tokens are something a person has and are external physical devices. The interface can be via the USB port and/or may require pre-install driver code. Tokens support multiple authentication technologies and have the ability to run their own specialized programs. Technology solutions include generated unique pass-codes, e.g., random 6-digit number that changes every minute; biometric data, e.g. fingerprint (hash); or a digital certificate.

Keystroke recognition

Keystroke recognition—something a person is—is a biometric technique that rates the flow of movement to measure data entry on a computer keyboard. Post measurements are compared to a pre-recorded baseline. Biometric solutions authenticate the identity on the basis of a physiological or physical characteristic. Keystroke, as with other biometric methods require some overhead during the initial contact to establish a baseline measurement.

Digital Certificate

Digital certificates are something a person has and are represented by a file on a local machine or token. Certificates can contain a person’s organization, name, proprietary data and a cryptograph public key. Certificates are very useful when authentication and electronic signatures are functional requirements.

User Applications

Depending on the business needs, strong authentication can be applied at many levels in the organization. The usage can include, but is not limited to:

- Customer/consumer – eCommerce online users
- Business partner
- Employee – remote connectivity
- Enterprise – internal strong authentication
- IT department – system administrators with privileged rights

The same strong authentication solution can be applied to combinations of usage scenarios. The nature of applications is that applications drive their own set of risks and requirements. The best guidance is to fall back on general risk mitigation practices: understand the assets utilized by the application; be familiar with the architecture, both internal and external; and finally, identify the threats and vulnerabilities that potentially can have an adverse impact on your business.

Education

There are many reasons to implement strong authentication solutions in the organization. For example, organizations may face regulatory requirements or business requirements for data protection, peace of mind and public relations.

When a solution is identified and deployed, it is imperative to provide awareness on the reasons for the new authentication methods. Training programs will help explain why two or more pieces of information are required to logon and what risks or liabilities you are protecting. Regardless of the type of users who will use the technology, awareness and user training programs are always necessary for a successful implementation of new technology and process.

Future Actions

Step One: Identify the Pieces

While it may seem like an obvious place to start, identification of the various Internet pieces is a must. Document not only the websites, but the information that is collected, the transactions that are allowed, and the interfaces that may be included in the architecture. Do not limit your assessment to just Business-to-Customer (B-C) sites, but include Business-to-Business (B-B) sites as well. Good site diagrams and architectural diagrams will help in both the assessment and reporting phases of the process. Lastly, be sure to document all cases where users can submit or retrieve information that is stored in back-end databases or systems.

Step Two: Assign Risk Value

The next step is to assign a risk value to each of the sites, data elements, and inter-connections identified in the first phase. How this is done and what scale is used is up to each company, but it is important that you are consistent and have supporting documentation to validate your assignments.

Step Three: Identify Mitigating Controls

There are other things that you are doing to mitigate risk other than usernames and passwords (or at least you should be!) Identify and document the audit, quality control, off line, and other processes that you have in place that mitigate the risk associated with your online endeavors. Mitigating controls can be anything that limit the ability for an unauthorized party to access or obtain the customer information.

Step Four: Determine Likelihood and Impact

This is probably the most difficult step of the process because it requires the assessor to take an honest look at their risk exposure and in some cases identify areas where they have not adequately performed their duties. In many organizations, especially those with smaller IT departments, the people with the skill and understanding of today's risks are the same ones responsible for protecting the company against them. Asking them to determine the likelihood and impact of a risk is asking them to identify areas in their jobs where they have been less than successful. Employing a third party or having a group analyze this step is a good approach to overcoming this natural tendency.

Step Five: Do you need to move beyond Username/password?

The next step in this process is to compare the items in the first four steps to determine if you have areas of sensitive data or access that also have an above average likelihood of exposure or impact. While each company has to determine the level of risk and exposure they are comfortable with, the FFIEC has already stated that authentication with just a username and password is not adequate for systems that grant access to non-public customer information or allow for the transfer of funds to third parties. However, just like with step two, it is vital that each company document the reasoning for the conclusions they come up with. It will save hours of debate with auditors if you already have documented and approved the reasoning and justification behind your decisions.

Step Six: Implement a two-factor solution for your high risk areas?

The last step in this process is to implement a two-factor authentication solution for your high risk areas. Implementing the solution includes the deployment of the strong authentication solution you selected, communication and awareness training for your employees, users, business partners, etc., and ongoing maintenance of the solution.

References

[MBA Information Security Resource Center](#) is a source of security content and references outlining MBA activities with advocacy, education and guidance.

[MBA Data Security Task Force policy recommendations](#) summarizes 10 areas of data privacy advocacy with narratives and recommendations for the industry.

[5-Step IA Model for Mortgage Industry Institutions](#) paper consist of research and analysis of applicable legislation, regulations, audit practices, and security standards to formulate a harmonized information assurance model for the mortgage industry.

[Global Data Protection Laws](#) provides an overview of global data protect laws.

Security Identity Services Accreditation Corporation ([SISAC](#)) represents industry best practices and policies for Public Key Infrastructure (PKI) strong authentication. This venue is designed to achieve regulatory requirements and interoperability, while providing a level playing field for all participants.

MISMO [Information Security Workgroup \(ISWG\) landing page](#) supports the information security concerns of other MISMO workgroups, provide industry security related recommendations, and general security educational material.

[Identifying and Safeguarding Personal Information](#) white paper from the MISMO Information Security Workgroup (ISWG) on state security breach legislation, guidelines and practices.

[FFIEC - Authentication in an Internet Banking Environment](#)

[FFIEC Information Technology Examination Handbook – Information Security](#)

[Frequently Asked Questions on *FFIEC Guidance on Authentication in an Internet Banking Environment*](#)

[NIST Special Publication 800-63 - Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology](#)