BOARD OF GOVERNORS

OF THE

FEDERAL RESERVE SYSTEM

WASHINGTON, D.C. 20551

DIVISION OF BANKING
SUPERVISION AND REGULATION

SR 05 - 19

October 13, 2005

TO THE OFFICER IN CHARGE OF SUPERVISION AND APPROPRIATE SUPERVISORY AND EXAMINATION STAFF AT EACH FEDERAL RESERVE BANK, AND TO BANKING ORGANIZATIONS SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: Interagency Guidance on Authentication in an Internet Banking Environment

The Federal Financial Institutions Examination Council (FFIEC) has issued the attached guidance titled *Authentication in an Internet Banking Environment.* This guidance updates and replaces the FFIEC's *Authentication in an Electronic Banking Environment* issued in 2001 and specifically addresses the need for risk-based assessments, customer awareness, and security measures to reliably authenticate customers accessing financial institutions' Internet-based services. The guidance also emphasizes that the agencies consider single-factor authentication, if it is the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a technology service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Consistent with the FFIEC's *Information Security Booklet* (December 2002), which is incorporated in the *Information Technology Examination Handbook,* financial institutions should periodically:

- Ensure that their information security programs:
    - Identify and assess the risks associated with the full range of Internet-based products and services,
    - Identify risk mitigation actions, including appropriate measures to verify and authenticate customers, and

- Measure and evaluate customer awareness efforts;

- Establish, evaluate, and adjust, as appropriate, their information security programs in light of any relevant changes in technology, the sensitivity of their customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Examiners should begin to assess financial institutions' progress in meeting the expectations outlined in the guidance and thereafter monitor ongoing conformance as needed during the risk-focused examination process. Financial institutions will be expected to have achieved conformance with the guidance by year-end 2006. Examiners should document situations where financial institutions have not achieved conformance with the guidance by that time.

Federal Reserve Banks are asked to distribute this letter and the interagency guidance to banking organizations supervised by the Federal Reserve, as well as to their supervisory and examination staff. If you have any questions concerning this guidance, please contact Stacy Coleman, Assistant Director, Operational and IT Risk Section, at (202) 452-2934 or Elton Hill, Senior Supervisory Financial Analyst, at (202) 452-2514.

Richard Spillenkothen
Director

Attachment: *Authentication in an Internet Banking Environment*

Supercede: FFIEC Guidance on Authentication (SR 01-20 (SUP))

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;[2] increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;

- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information,[3] to prevent money laundering and terrorist financing,[4] to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. (The appendix to this guidance contains a more detailed discussion of authentication techniques.) The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

---

[3] The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule.

[4] The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).

Existing authentication methodologies involve three basic "factors":

- Something the user ***knows*** (e.g., password, PIN);
- Something the user ***has*** (e.g., ATM card, smart card); and
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band"[5] controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and "layered" approach to information security.[6]

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting

---

[5] Out–of–band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cell–phone based challenge/ response processes are some examples.

[6] *FFIEC Information Technology Examination Handbook,* Information Security Booklet, December 2002; *FFIEC Information Technology Examination Handbook,* E-Banking Booklet, August 2003.

selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming,[7] malware,[8] and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The risk assessment process should:

- Identify all transactions and levels of access associated with Internet-based customer products and services;

- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and

- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Moreover, customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons.

---

[7] Similar in nature to e-mail phishing, pharming seeks to obtain personal information by directing users to spoofed Web sites where their information is captured, usually from a legitimate–looking form.

[8] Short for *malicious software,* such as software designed to capture and forward private information such as ID's, passwords, account numbers, and PINs.

One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods. (The appendix to this guidance describes verification processes in more detail.)

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. In addition, financial institutions should report suspicious activities to appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.[9]

Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access. Furthermore, if critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the institution in a timely manner. An independent party (e.g., internal or external auditor) should review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program

[9] 31 USC 5318; 12 CFR 21.11 (OCC); 12 CFR 563.180 (OTS); 12 CFR 353 (FDIC); 12 CFR 208.62 [state member banks]; 12 CFR 211.5 (k) [edge or agreement corporation, or any branch or subsidiary thereof]; 12 CFR 211.24 (f) [uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States]; 12 CFR 225.4 (f) [bank holding company or any non bank subsidiary thereof] (FRB); and 12 CFR Part 748.1 and Part 748.2 (NCUA).

and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Conclusion

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Appendix[10]

Background

The term *authentication*, as used in this guidance, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication process is one method used to control access to customer accounts and personal information. Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

Customer identifiers may be a bankcard for ATM usage, or some form of user ID for remote access. An authentication factor (e.g. PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. Single-factor authentication involves the use of one factor to verify customer identity. The most common single-factor method is the use of a password. Two-factor authentication is most widely used with ATMs. To withdraw money from an ATM, the customer must present both an ATM card (*something the person has*) and a password or PIN (*something the person knows*). Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations. The effectiveness of a particular authentication technique is dependent upon the integrity of the selected product or process and the manner in which it is implemented and managed.

---

[10] This Appendix is based upon the FDIC Study – "Putting an End to Account-Hijacking Identity Theft" (December 14, 2004) and the FDIC Study Supplement (June 17, 2005).

Authentication Techniques, Processes, and Methodologies

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

Shared Secrets

Shared secrets (*something a person knows)* are information elements that are known or shared by both the customer and the authenticating entity. Passwords and PINs are the best known shared secret techniques but some new and different types are now being used as well. Some additional examples are:

- Questions or queries that require specific customer knowledge to answer, e.g., the exact amount of the customer's monthly mortgage payment.

- Customer-selected images that must be identified or selected from a pool of images.

The customer's selection of a shared secret normally occurs during the initial enrollment process or via an offline ancillary process. Passwords or PIN values can be chosen, questions can be chosen and responses provided, and images may be uploaded or selected.

The security of shared secret processes can be enhanced with the requirement for periodic change. Shared secrets that never change are described as "static" and the risk of compromise increases over time. The use of multiple shared secrets also provides increased security because more than one secret must be known to authenticate.

Shared secrets can also be used to authenticate the institution's Web site to the customer. This is discussed in the Mutual Authentication section.

Tokens

Tokens are physical devices (*something the person has)* and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

<u>USB Token Device</u>

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

Password-Generating Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if (1) the regular password matches and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*).

Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition;
- face recognition;
- voice recognition;
- keystroke recognition;
- handwriting recognition;
- finger and hand geometry;
- retinal scan; and
- iris scan.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition.

Fingerprint Recognition

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data extracted from fingerprints are extremely dense and the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification.[11]

Although end users should have little trouble using a fingerprint-scanning device, special hardware and software must be installed on the user's computer. Fingerprint recognition implementation will vary according to the vendor and the degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user's computer. However, fingerprint biometrics is generally considered easier

[11] Currently, some financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, are eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

to install and use than other, more complex technologies, such as iris scanning. Enrollment can be performed either at the financial institution's customer service center or remotely by the customer after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution should consider requiring that customers appear in person.

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called "mug shot" environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Non-Hardware-Based One-Time-Password Scratch Card

Scratch cards (*something a person has*) are less-expensive, "low-tech" versions of the OTP generating tokens discussed previously. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

Used in a multifactor authentication process, the customer first enters his or her user name and password in the established manner. Assuming the information is input correctly, the customer will then be asked to input, as a second authentication factor, the characters contained in a randomly chosen cell in the grid. The customer will respond by typing in the data contained in the grid cell element that corresponds to the challenge coordinates.

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Out-of-Band Authentication

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests,

purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

Internet Protocol Address (IPA) Location and Geo-Location

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned, may change frequently, and in some cases can be "spoofed." Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable

results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet such as cellular/digital telephones.

Mutual Authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increasing level of confidence that the applicant is who they say they are.

- *Logical verification* to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf are not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Another authentication method consists of the financial institution relying on a third party to verify the identity of the applicant. The third party would issue the applicant an electronic credential, such as a digital certificate, that can be used by the applicant to prove his/her identity. The financial institution is responsible for ensuring that the third party uses the same level of authentication that the financial institution would use itself.

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;[2] increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;

- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information,[3] to prevent money laundering and terrorist financing,[4] to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. (The appendix to this guidance contains a more detailed discussion of authentication techniques.) The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

---

[3] The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule.

[4] The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).

Existing authentication methodologies involve three basic "factors":

- Something the user ***knows*** (e.g., password, PIN);
- Something the user ***has*** (e.g., ATM card, smart card); and
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band"[5] controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and "layered" approach to information security.[6]

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting

---

[5] Out–of–band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cell–phone based challenge/ response processes are some examples.

[6] *FFIEC Information Technology Examination Handbook,* Information Security Booklet, December 2002; *FFIEC Information Technology Examination Handbook,* E-Banking Booklet, August 2003.

selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming,[7] malware,[8] and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The risk assessment process should:

- Identify all transactions and levels of access associated with Internet-based customer products and services;

- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and

- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Moreover, customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons.

---

[7] Similar in nature to e-mail phishing, pharming seeks to obtain personal information by directing users to spoofed Web sites where their information is captured, usually from a legitimate–looking form.

[8] Short for *malicious software,* such as software designed to capture and forward private information such as ID's, passwords, account numbers, and PINs.

One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods. (The appendix to this guidance describes verification processes in more detail.)

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. In addition, financial institutions should report suspicious activities to appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.[9]

Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access. Furthermore, if critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the institution in a timely manner. An independent party (e.g., internal or external auditor) should review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program

[9] 31 USC 5318; 12 CFR 21.11 (OCC); 12 CFR 563.180 (OTS); 12 CFR 353 (FDIC); 12 CFR 208.62 [state member banks]; 12 CFR 211.5 (k) [edge or agreement corporation, or any branch or subsidiary thereof]; 12 CFR 211.24 (f) [uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States]; 12 CFR 225.4 (f) [bank holding company or any non bank subsidiary thereof] (FRB); and 12 CFR Part 748.1 and Part 748.2 (NCUA).

and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Conclusion

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Appendix[10]

Background

The term *authentication*, as used in this guidance, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication process is one method used to control access to customer accounts and personal information. Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

Customer identifiers may be a bankcard for ATM usage, or some form of user ID for remote access. An authentication factor (e.g. PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. Single-factor authentication involves the use of one factor to verify customer identity. The most common single-factor method is the use of a password. Two-factor authentication is most widely used with ATMs. To withdraw money from an ATM, the customer must present both an ATM card (*something the person has*) and a password or PIN (*something the person knows*). Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations. The effectiveness of a particular authentication technique is dependent upon the integrity of the selected product or process and the manner in which it is implemented and managed.

---

[10] This Appendix is based upon the FDIC Study – "Putting an End to Account-Hijacking Identity Theft" (December 14, 2004) and the FDIC Study Supplement (June 17, 2005).

Authentication Techniques, Processes, and Methodologies

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

Shared Secrets

Shared secrets (*something a person knows)* are information elements that are known or shared by both the customer and the authenticating entity. Passwords and PINs are the best known shared secret techniques but some new and different types are now being used as well. Some additional examples are:

- Questions or queries that require specific customer knowledge to answer, e.g., the exact amount of the customer's monthly mortgage payment.

- Customer-selected images that must be identified or selected from a pool of images.

The customer's selection of a shared secret normally occurs during the initial enrollment process or via an offline ancillary process. Passwords or PIN values can be chosen, questions can be chosen and responses provided, and images may be uploaded or selected.

The security of shared secret processes can be enhanced with the requirement for periodic change. Shared secrets that never change are described as "static" and the risk of compromise increases over time. The use of multiple shared secrets also provides increased security because more than one secret must be known to authenticate.

Shared secrets can also be used to authenticate the institution's Web site to the customer. This is discussed in the Mutual Authentication section.

Tokens

Tokens are physical devices (*something the person has)* and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

<u>USB Token Device</u>

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

Password-Generating Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if (1) the regular password matches and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*).

Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition;
- face recognition;
- voice recognition;
- keystroke recognition;
- handwriting recognition;
- finger and hand geometry;
- retinal scan; and
- iris scan.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition.

Fingerprint Recognition

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data extracted from fingerprints are extremely dense and the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification.[11]

Although end users should have little trouble using a fingerprint-scanning device, special hardware and software must be installed on the user's computer. Fingerprint recognition implementation will vary according to the vendor and the degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user's computer. However, fingerprint biometrics is generally considered easier

[11] Currently, some financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, are eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

to install and use than other, more complex technologies, such as iris scanning. Enrollment can be performed either at the financial institution's customer service center or remotely by the customer after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution should consider requiring that customers appear in person.

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called "mug shot" environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Non-Hardware-Based One-Time-Password Scratch Card

Scratch cards (*something a person has*) are less-expensive, "low-tech" versions of the OTP generating tokens discussed previously. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

Used in a multifactor authentication process, the customer first enters his or her user name and password in the established manner. Assuming the information is input correctly, the customer will then be asked to input, as a second authentication factor, the characters contained in a randomly chosen cell in the grid. The customer will respond by typing in the data contained in the grid cell element that corresponds to the challenge coordinates.

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Out-of-Band Authentication

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests,

purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

Internet Protocol Address (IPA) Location and Geo-Location

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned, may change frequently, and in some cases can be "spoofed." Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable

results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet such as cellular/digital telephones.

Mutual Authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increasing level of confidence that the applicant is who they say they are.

- *Logical verification* to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf are not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Another authentication method consists of the financial institution relying on a third party to verify the identity of the applicant. The third party would issue the applicant an electronic credential, such as a digital certificate, that can be used by the applicant to prove his/her identity. The financial institution is responsible for ensuring that the third party uses the same level of authentication that the financial institution would use itself.

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;[2] increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;

- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information,[3] to prevent money laundering and terrorist financing,[4] to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. (The appendix to this guidance contains a more detailed discussion of authentication techniques.) The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

---

[3] The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule.

[4] The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).

Existing authentication methodologies involve three basic "factors":

- Something the user ***knows*** (e.g., password, PIN);
- Something the user ***has*** (e.g., ATM card, smart card); and
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band"[5] controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and "layered" approach to information security.[6]

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting

---

[5] Out–of–band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cell–phone based challenge/ response processes are some examples.

[6] *FFIEC Information Technology Examination Handbook,* Information Security Booklet, December 2002; *FFIEC Information Technology Examination Handbook,* E-Banking Booklet, August 2003.

selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming,[7] malware,[8] and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The risk assessment process should:

- Identify all transactions and levels of access associated with Internet-based customer products and services;

- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and

- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Moreover, customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons.

---

[7] Similar in nature to e-mail phishing, pharming seeks to obtain personal information by directing users to spoofed Web sites where their information is captured, usually from a legitimate–looking form.

[8] Short for *malicious software,* such as software designed to capture and forward private information such as ID's, passwords, account numbers, and PINs.

One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods. (The appendix to this guidance describes verification processes in more detail.)

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. In addition, financial institutions should report suspicious activities to appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.[9]

Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access. Furthermore, if critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the institution in a timely manner. An independent party (e.g., internal or external auditor) should review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program

[9] 31 USC 5318; 12 CFR 21.11 (OCC); 12 CFR 563.180 (OTS); 12 CFR 353 (FDIC); 12 CFR 208.62 [state member banks]; 12 CFR 211.5 (k) [edge or agreement corporation, or any branch or subsidiary thereof]; 12 CFR 211.24 (f) [uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States]; 12 CFR 225.4 (f) [bank holding company or any non bank subsidiary thereof] (FRB); and 12 CFR Part 748.1 and Part 748.2 (NCUA).

and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Conclusion

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Appendix[10]

Background

The term *authentication*, as used in this guidance, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication process is one method used to control access to customer accounts and personal information. Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

Customer identifiers may be a bankcard for ATM usage, or some form of user ID for remote access. An authentication factor (e.g. PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. Single-factor authentication involves the use of one factor to verify customer identity. The most common single-factor method is the use of a password. Two-factor authentication is most widely used with ATMs. To withdraw money from an ATM, the customer must present both an ATM card (*something the person has*) and a password or PIN (*something the person knows*). Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations. The effectiveness of a particular authentication technique is dependent upon the integrity of the selected product or process and the manner in which it is implemented and managed.

---

[10] This Appendix is based upon the FDIC Study – "Putting an End to Account-Hijacking Identity Theft" (December 14, 2004) and the FDIC Study Supplement (June 17, 2005).

Authentication Techniques, Processes, and Methodologies

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

Shared Secrets

Shared secrets (*something a person knows)* are information elements that are known or shared by both the customer and the authenticating entity. Passwords and PINs are the best known shared secret techniques but some new and different types are now being used as well. Some additional examples are:

- Questions or queries that require specific customer knowledge to answer, e.g., the exact amount of the customer's monthly mortgage payment.

- Customer-selected images that must be identified or selected from a pool of images.

The customer's selection of a shared secret normally occurs during the initial enrollment process or via an offline ancillary process. Passwords or PIN values can be chosen, questions can be chosen and responses provided, and images may be uploaded or selected.

The security of shared secret processes can be enhanced with the requirement for periodic change. Shared secrets that never change are described as "static" and the risk of compromise increases over time. The use of multiple shared secrets also provides increased security because more than one secret must be known to authenticate.

Shared secrets can also be used to authenticate the institution's Web site to the customer. This is discussed in the Mutual Authentication section.

Tokens

Tokens are physical devices (*something the person has)* and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

<u>USB Token Device</u>

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

Password-Generating Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if (1) the regular password matches and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*).

Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition;
- face recognition;
- voice recognition;
- keystroke recognition;
- handwriting recognition;
- finger and hand geometry;
- retinal scan; and
- iris scan.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition.

Fingerprint Recognition

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data extracted from fingerprints are extremely dense and the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification.[11]

Although end users should have little trouble using a fingerprint-scanning device, special hardware and software must be installed on the user's computer. Fingerprint recognition implementation will vary according to the vendor and the degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user's computer. However, fingerprint biometrics is generally considered easier

[11] Currently, some financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, are eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

to install and use than other, more complex technologies, such as iris scanning. Enrollment can be performed either at the financial institution's customer service center or remotely by the customer after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution should consider requiring that customers appear in person.

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called "mug shot" environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Non-Hardware-Based One-Time-Password Scratch Card

Scratch cards (*something a person has*) are less-expensive, "low-tech" versions of the OTP generating tokens discussed previously. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

Used in a multifactor authentication process, the customer first enters his or her user name and password in the established manner. Assuming the information is input correctly, the customer will then be asked to input, as a second authentication factor, the characters contained in a randomly chosen cell in the grid. The customer will respond by typing in the data contained in the grid cell element that corresponds to the challenge coordinates.

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Out-of-Band Authentication

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests,

purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

Internet Protocol Address (IPA) Location and Geo-Location

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned, may change frequently, and in some cases can be "spoofed." Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable

results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet such as cellular/digital telephones.

Mutual Authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increasing level of confidence that the applicant is who they say they are.

- *Logical verification* to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf are not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Another authentication method consists of the financial institution relying on a third party to verify the identity of the applicant. The third party would issue the applicant an electronic credential, such as a digital certificate, that can be used by the applicant to prove his/her identity. The financial institution is responsible for ensuring that the third party uses the same level of authentication that the financial institution would use itself.

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;[2] increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;

- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information,[3] to prevent money laundering and terrorist financing,[4] to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. (The appendix to this guidance contains a more detailed discussion of authentication techniques.) The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

---

[3] The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule.

[4] The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).

Existing authentication methodologies involve three basic "factors":

- Something the user ***knows*** (e.g., password, PIN);
- Something the user ***has*** (e.g., ATM card, smart card); and
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band"[5] controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and "layered" approach to information security.[6]

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting

---

[5] Out–of–band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cell–phone based challenge/ response processes are some examples.

[6] *FFIEC Information Technology Examination Handbook,* Information Security Booklet, December 2002; *FFIEC Information Technology Examination Handbook,* E-Banking Booklet, August 2003.

selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming,[7] malware,[8] and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The risk assessment process should:

- Identify all transactions and levels of access associated with Internet-based customer products and services;

- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and

- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Moreover, customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels because of the absence of the physical cues that financial institutions traditionally use to identify persons.

---

[7] Similar in nature to e-mail phishing, pharming seeks to obtain personal information by directing users to spoofed Web sites where their information is captured, usually from a legitimate–looking form.

[8] Short for *malicious software,* such as software designed to capture and forward private information such as ID's, passwords, account numbers, and PINs.

One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods. (The appendix to this guidance describes verification processes in more detail.)

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. In addition, financial institutions should report suspicious activities to appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.[9]

Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access. Furthermore, if critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the institution in a timely manner. An independent party (e.g., internal or external auditor) should review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft, financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program

[9] 31 USC 5318; 12 CFR 21.11 (OCC); 12 CFR 563.180 (OTS); 12 CFR 353 (FDIC); 12 CFR 208.62 [state member banks]; 12 CFR 211.5 (k) [edge or agreement corporation, or any branch or subsidiary thereof]; 12 CFR 211.24 (f) [uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States]; 12 CFR 225.4 (f) [bank holding company or any non bank subsidiary thereof] (FRB); and 12 CFR Part 748.1 and Part 748.2 (NCUA).

and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Conclusion

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Appendix[10]

Background

The term *authentication*, as used in this guidance, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication process is one method used to control access to customer accounts and personal information. Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

Customer identifiers may be a bankcard for ATM usage, or some form of user ID for remote access. An authentication factor (e.g. PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. Single-factor authentication involves the use of one factor to verify customer identity. The most common single-factor method is the use of a password. Two-factor authentication is most widely used with ATMs. To withdraw money from an ATM, the customer must present both an ATM card (*something the person has*) and a password or PIN (*something the person knows*). Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations. The effectiveness of a particular authentication technique is dependent upon the integrity of the selected product or process and the manner in which it is implemented and managed.

---

[10] This Appendix is based upon the FDIC Study – "Putting an End to Account-Hijacking Identity Theft" (December 14, 2004) and the FDIC Study Supplement (June 17, 2005).

Authentication Techniques, Processes, and Methodologies

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

Shared Secrets

Shared secrets (*something a person knows)* are information elements that are known or shared by both the customer and the authenticating entity. Passwords and PINs are the best known shared secret techniques but some new and different types are now being used as well. Some additional examples are:

- Questions or queries that require specific customer knowledge to answer, e.g., the exact amount of the customer's monthly mortgage payment.

- Customer-selected images that must be identified or selected from a pool of images.

The customer's selection of a shared secret normally occurs during the initial enrollment process or via an offline ancillary process. Passwords or PIN values can be chosen, questions can be chosen and responses provided, and images may be uploaded or selected.

The security of shared secret processes can be enhanced with the requirement for periodic change. Shared secrets that never change are described as "static" and the risk of compromise increases over time. The use of multiple shared secrets also provides increased security because more than one secret must be known to authenticate.

Shared secrets can also be used to authenticate the institution's Web site to the customer. This is discussed in the Mutual Authentication section.

Tokens

Tokens are physical devices (*something the person has)* and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

<u>USB Token Device</u>

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

Password-Generating Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if (1) the regular password matches and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person know*s) or a token (*something a person has*).

Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition;
- face recognition;
- voice recognition;
- keystroke recognition;
- handwriting recognition;
- finger and hand geometry;
- retinal scan; and
- iris scan.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition.

Fingerprint Recognition

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data extracted from fingerprints are extremely dense and the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification.[11]

Although end users should have little trouble using a fingerprint-scanning device, special hardware and software must be installed on the user's computer. Fingerprint recognition implementation will vary according to the vendor and the degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user's computer. However, fingerprint biometrics is generally considered easier

[11] Currently, some financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, are eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

to install and use than other, more complex technologies, such as iris scanning. Enrollment can be performed either at the financial institution's customer service center or remotely by the customer after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution should consider requiring that customers appear in person.

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called "mug shot" environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Non-Hardware-Based One-Time-Password Scratch Card

Scratch cards (*something a person has*) are less-expensive, "low-tech" versions of the OTP generating tokens discussed previously. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

Used in a multifactor authentication process, the customer first enters his or her user name and password in the established manner. Assuming the information is input correctly, the customer will then be asked to input, as a second authentication factor, the characters contained in a randomly chosen cell in the grid. The customer will respond by typing in the data contained in the grid cell element that corresponds to the challenge coordinates.

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Out-of-Band Authentication

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests,

purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

Internet Protocol Address (IPA) Location and Geo-Location

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned, may change frequently, and in some cases can be "spoofed." Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable

results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet such as cellular/digital telephones.

Mutual Authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increasing level of confidence that the applicant is who they say they are.

- *Logical verification* to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf are not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Another authentication method consists of the financial institution relying on a third party to verify the identity of the applicant. The third party would issue the applicant an electronic credential, such as a digital certificate, that can be used by the applicant to prove his/her identity. The financial institution is responsible for ensuring that the third party uses the same level of authentication that the financial institution would use itself.