NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: August 2001 **LETTER NO.: 01-CU-10**

TO: Federally Insured Credit Unions

SUBJ: Authentication in an Electronic Banking Environment

ENCL: FFIEC Guidance on Authentication in an Electronic Banking Environment

The purpose of this letter is to make you aware of guidance recently released by the Federal Financial Institutions Examination Council ("FFIEC") [1] to financial institutions regarding authenticating users in an electronic banking environment. If your credit union offers, or is planning to offer, internet-based electronic financial services to your members, I encourage you to carefully review the enclosed FFIEC guidance paper.

Member interaction with credit unions is migrating from paper-based transactions to remote electronic access and transaction initiation. This migration increases the risk of doing business with unauthorized or incorrectly identified parties that could result in financial loss or reputation damage to the credit union. When properly implemented, authentication can help credit unions reduce fraud and promote legal enforceability of electronic agreements and transactions.

An effective authentication program should be implemented across a credit union's operations and the level of authentication used in a particular application should be appropriate to the level of risk in that application. In short, the success of a particular authentication program depends not only on technology, but also on effective policies, procedures, and controls. The paper emphasizes the following points:

- ✓ The credit union's authentication process should be consistent and support the credit union's overall security and risk assessment programs. Further, the implementation of appropriate authentication methodologies starts with an enterprise-wide assessment of the risk posed by the credit union's electronic banking systems.

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

- ✓ Credit unions need to utilize reliable methods to verify the identity of members during the account origination process, as well as authenticating members before granting them access to on-line banking systems.

- ✓ A sound authentication system should include audit and monitoring features that can assist in detecting fraud, unusual activities, compromised passwords, or other unauthorized activities.

- ✓ The credit union's authentication process should be reviewed periodically to assess the adequacy of existing authentication techniques in light of changing or new risks.

If you have any questions or concerns, please contact your examiner, NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

Dennis Dollar
Acting Chairman

Enclosure

Federal Financial Institutions Examination Council

2000 K Street, NW, Suite 310 . Washington, DC 20006 . (202) 872-7500 . FAX (202) 872-7501

Authentication in an Electronic Banking Environment
August 8, 2001

Purpose

This interagency guidance focuses on the risks and risk management controls related to authentication in an electronic banking environment. It reviews the risks and risk management controls of a number of existing and emerging authentication tools necessary to initially *verify* the identity of new customers and *authenticate* existing customers that access electronic banking services. These functions are jointly referred to as "authentication" in this guidance.

This guidance applies to both retail and commercial customers and is intended to be "technology neutral." Financial institutions may use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a third party service provider.[1] Furthermore, management should review this guidance in conjunction with other guidance to ensure that safety and soundness objectives concerning confidentiality, data integrity, contract enforceability, and effective internal controls are adequately addressed. Financial institutions may also consider this guidance in implementing certain elements of the recently issued Guidelines Establishing Standards for Safeguarding Customer Information.[2]

Background

Reliable customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. An effective authentication system can help financial institutions reduce fraud and promote the legal enforceability of their electronic agreements and transactions. Strong customer authentication practices also are necessary to enforce anti-money laundering measures and help financial institutions detect and reduce identity theft.[3] Customer interaction with financial institutions is migrating from physical recognition and paper-based

[1] This guidance focuses on authenticating financial institution customers accessing institution computer systems via the Internet. However, its principles are also applicable to the authentication of institution employees and contractors attempting to access any networked institution computer system.

[2] The Interagency Guidelines for Safeguarding Customer Information (66 Federal Register 8616, February 1, 2001 - OCC, FDIC, FRB, OTS and 66 Federal Register 8152, January 30, 2001 – NCUA) describes the general process that financial institutions should use to protect customer information.

[3] Identity theft is the use of another individual's name, social security number, or other personal information to obtain financial services. A crime under 18 U.S.C. 1028, identity theft occurs when someone impersonates a legitimate customer in order to defraud a financial institution or its customers. Perpetrators can obtain personal information in a variety of ways. The OCC, FDIC, FRB and OTS recently issued guidance on identity theft. The NCUA plans to issue similar guidance in the near future. In addition, the Federal Trade Commission has published guidance on preventing identity theft. Information is available at http://www.consumer.gov/idtheft.

documentation to remote electronic access and transaction initiation. The risks of doing business with unauthorized or incorrectly identified individuals in an electronic banking environment could result in financial loss and reputation damage through fraud, disclosure of confidential information, corruption of data or unenforceable agreements.

There are a variety of authentication tools and methodologies financial institutions can use to authenticate customers. These include the use of passwords and personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards or other types of "tokens," database comparisons, and biometric identifiers. (The Appendix contains a more detailed discussion of authentication methods.) The level of risk protection afforded by each of these tools varies and is evolving as technology changes.

Existing authentication methodologies involve three basic "factors":

- something the user ***knows*** (e.g., password, PIN);
- something the user ***possesses*** (e.g., ATM card, smart card); and
- something the user ***is*** (e.g., biometric characteristic, such as a fingerprint or retinal pattern).

Authentication methods that depend on more than one factor typically are more difficult to compromise than single factor systems. Accordingly, properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents. For example, the use of a logon ID/password is single factor authentication (i.e., something the user knows); whereas, a transaction using an ATM typically requires two-factor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). In general, multi-factor authentication methods should be used on higher risk systems. Further, institutions should be sensitive to the fact that proper implementation is key to the reliability and security of any authentication system. For example, a poorly implemented two-factor system may be less secure than a properly implemented single-factor system.

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

An effective authentication program should be implemented on an enterprise-wide basis to ensure that controls and authentication tools are adequate among products, services, and lines of business. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for electronic banking and e-commerce customer services. The agencies believe the level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

The implementation of appropriate authentication methodologies starts with an assessment of the risk posed by the institution's electronic banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the institution's transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity and value of the stored information to both the institution and the customer; the ease of using the method; and the size and volume of transactions.

An enterprise-wide approach to authentication requires development of and adherence to corporate standards and architecture, integration of authentication processes within the overall information security framework, risk assessments within lines of businesses supporting selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific electronic application should be appropriate and "commercially reasonable" 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 service providers should periodically review authentication technology and ensure appropriate changes are implemented.

Single factor authentication tools, including passwords and PINs, have been widely accepted as commercially reasonable for a variety of retail e-banking activities, including account inquiry, bill payment and account aggregation. However, financial institutions should assess the adequacy of existing authentication techniques in light of changing or new risks (e.g., increasing ability of hackers to compromise less robust single factor techniques). The agencies caution financial institutions that single factor authentication alone may not be commercially reasonable or adequate for high risk applications and transactions. Instead, multi-factor techniques may be necessary. Institutions should recognize that a single factor system may be "tiered" to enhance security without implementing a two-factor system. A tiered single factor authentication system would include the use of multiple levels of a single factor (e.g., the use of two or more passwords or PINs employed at different points in the authentication process).

In addition to limiting unauthorized access, effective authentication also provides institutions with a foundation to enforce electronic transactions and agreements. First, effective authentication provides the basis for *validation* of parties to the transaction and their agreement to its terms. Second, it is a necessary element to establish the *authenticity* of the records evidencing the electronic transaction should there ever be a dispute. Third, it is a necessary element to establish the *integrity* of the records evidencing the electronic transaction. All of these elements promote the enforceability of electronic agreements. Because state laws vary, management should involve legal counsel in the design and implementation of authentication systems.

Some uniform rules concerning the use of electronic signatures and records in retail and commercial transactions may emerge as a result of recent changes in federal law. While these changes provide more legal certainty that may help promote the growth of electronic commerce, federal law leaves unresolved several important issues related to the validity of an electronic record, as well as the verification and authorization of parties who conduct electronic transactions.[4] In addition, the Automated Clearing House (ACH) system is increasingly being

[4] See the Electronic Signatures in Global and National Commerce Act (E-Sign Act or Act), Pub. L. No. 106-229 (June 30, 2000). The E-Sign Act generally provides that a transaction is not invalid solely because an electronic signature was used with respect to a transaction in interstate or foreign commerce. The Act also generally provides that a record relating to such a transaction is not invalid solely because it is in electronic form. However, the Act does not resolve some important issues, such as the level of electronic signature technology that may be necessary for banks to meet safety and soundness standards when engaging in electronic transactions.

used as a payment system for funds transfers initiated on the Internet. The National Automated Clearing House Association has recently amended its operating rules concerning ACH funds transfers via the Internet. Financial institutions should be familiar with these new rules when designing and implementing their authentication system.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions need to utilize reliable methods of originating new customer accounts online. Customer identity verification during account origination 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 purely electronic channel because of the absence of the physical cues that bankers traditionally use to identify individuals.

One of the most reliable methods to verify a customer's identity is a face-to-face presentation of tangible proof of identity (e.g., driver's license). Similarly, to establish the validity of a business and the authority of individuals 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 electronic banking environment, reliance on these traditional forms of paper-based authentication is decreased substantially. Accordingly, financial institutions need to utilize reliable alternative methods.

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 applicants are 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 needed to establish an individual's right to act on a company's behalf (e.g., bylaws) 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.

Transaction Initiation and Authentication of Established Customers

Once a financial institution has successfully *verified* a customer's identity during the account origination process, it should *authenticate* customers who wish to gain access to the online banking system. Financial institutions can use a variety of methods to authenticate existing customers. These methods include the use of passwords, PINs, digital certificates and PKI, physical devices such as tokens, and biometrics.

Prudent controls promote the integrity of the authentication method. In addition, financial institutions can strengthen the reliability of the authentication methods by communicating customer responsibilities and recommended precautions. (Refer to the Appendix for a more detailed discussion on each of these authentication methods and prudent controls.)

Monitoring and Reporting

Monitoring systems can detect unauthorized access to computer systems and customer accounts. A sound authentication system should include audit features that can assist in the detection of fraud, unusual activities (e.g., 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 31 CFR 103.18.

Financial institutions may rely on multiple layers of controls to prevent fraud and safeguard customer information. Many of these controls are not based directly upon authentication. For example, a financial institution could analyze the typical transactional activity of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits for large items that require manual intervention to exceed the preset limit. In addition, financial institutions can monitor Internet Protocol (IP) addresses and other information to identify suspicious activity.

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 administrator's actions to provide the necessary checks and balances for managing system security.

Conclusion

Reliable electronic customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. The success of a particular authentication tool or methodology depends on more than the technology; it depends on appropriate policies, procedures and controls. An effective authentication method should be implemented on an enterprise-wide basis, have customer acceptance, reliable performance, scalability to

accommodate growth, and interoperability with existing systems and future plans. The agencies expect financial institutions to assess the risks to the institution and its customers and implement appropriate authentication methods in order to manage risk effectively. The level of authentication used by the financial institution in a particular application should be appropriate to the level of risk of that application.

Questions can be directed to:

Jeffrey M. Kopchik, Senior Policy Analyst, Division of Supervision, Technology Branch, FDIC at (202) 898-3872.
Matthew Biliouris, Information Systems Officer, Office of Examination & Insurance, NCUA at (703) 518-6394.
John Carlson, Senior Advisor, Bank Technology Division, OCC at (202) 874-5013.
Robert E. Engebreth, Director - Technology Risk Management, OTS at (202) 906-5631.
Michael Wallas, Supervisory Financial Analyst, Division of Banking Supervision and Regulation, FRB at (202) 452-2081

Appendix: Authentication Methods

Passwords and Personal Identification Numbers (PINs)

The most common authentication method for existing customers requesting access to electronic banking systems is the entry of a user name or ID and a secret string of characters such as a password or PIN. User IDs combined with passwords or PINs are considered a single-factor authentication technique. Popular acceptance of this form of authentication rests on its ease of use and its adaptability within existing infrastructures.

Financial institutions that allow customers to use passwords with short character length, readily identifiable words or dates, or widely used customer information (e.g., Social Security numbers) may be exposed to excessive risks in light of the increasing security threats from hackers and fraudulent insider abuse. Stronger security in password structure and implementation can help mitigate these risks. There are three aspects of passwords that contribute to the security they provide: secrecy, length and composition, and system controls.

Password secrecy. The security provided by password-only systems depends on the password being kept secret. If another party obtains the password, he or she can perform the same transactions as the intended user. Passwords can be compromised because of customer behavior or techniques that capture passwords as they travel over the Internet. Attackers can also use well-known weaknesses to gain access to a financial institution's (or its service provider's) Internet-connected systems and obtain password files. Because of these vulnerabilities, passwords and password files should be encrypted when stored or transmitted over open networks such as the Internet.

Financial institutions need to emphasize to customers the importance of protecting the password's confidentiality, cautioning customers against writing down passwords and preventing others from observing the entry of their passwords. Customers should log-off unattended computers that have been used to access on-line banking systems and invoke password protection over their screen savers. Passwords should be encrypted wherever stored or transmitted over open systems such as the Internet, and the system should prohibit any user, including the system or security administrator, from printing or viewing unencrypted passwords.

Password length and composition. The appropriate password length and composition depends on the value or sensitivity of the data protected by the password. Password composition standards that require numbers or symbols in the sequence of a password, in conjunction with both upper and lower case alphabetic characters, provide a stronger defense against password cracking programs. Selecting letters that do not create a common word but instead represent the first letter of each word in a favorite phrase, poem, or song (referred to as mnemonics) can create a memorable but difficult to crack password.

Systems linked to open networks like the Internet are subject to a greater number of individuals who may attempt to compromise the system. Attackers may use automated programs to systematically generate millions of alphanumeric combinations to learn a customer's password (i.e., brute force attack). A financial institution can reduce the risk of password compromise by communicating and enforcing prudent password selection and providing guidance to customers and employees.

System controls. When evaluating password-based electronic banking systems, management should consider whether the authentication system is consistent with the financial institution's security policy. This includes evaluating such areas as password length and composition requirements, incorrect logon lockout, password expiration, encryption requirements, and activity and exception report monitoring.

When utilizing password security measures, financial institutions need to consider the following:

- Selecting an adequate password length and composition that balances the ease of remembering the password with its vulnerability to compromise. The password length and composition requirements should be based on an analysis of the risks associated with the system(s) that the password is protecting, and whether or not the password is part of a single-factor or multi-factor authentication system. While the use of passwords/PINs with 4 or more characters is currently a common industry practice for retail systems, the industry is moving toward use of passwords of 6 characters with a combination of letters and numbers, which is particularly appropriate for single-factor authentication methods, to provide stronger protection against compromise;
- Restricting the use of automatic logon features;
- Locking users out after an excessive number of failed login attempts -- existing industry practice is no more than 5 incorrect attempts;
- Establishing an appropriate password expiration interval for sensitive internal or high-value systems;
- Establishing strong procedures for disabling passwords after a prolonged period of inactivity;
- Implementing a secure process for password generation and distribution;
- Terminating customer connections after a specified interval of inactivity-- Industry practice is generally not more than 20 to 30 minutes;
- Establishing strong procedures for password resets and maintaining customer confidentiality of the password by forcing a password change at the next logon;
- Reviewing password exception reports;
- Applying strong and secure access controls over password databases;
- Providing guidance to customers and employees on prudent password selection and the importance of protecting the password's confidentiality;
- Discouraging the use of widely available customer identifiers (e.g., Social Security numbers) as passwords or user identifications; and
- Incorporating a multi-factor authentication method for sensitive internal or high-value systems.

Digital Certificates using Public Key Infrastructure (PKI)

A financial institution may use a PKI system to authenticate customers to its own electronic banking product. Institutions may also use the infrastructure to provide authentication services to customers who wish to transact business over the Internet with other entities or to identify employees and commercial partners seeking access to the business's internal systems. This guidance focuses on the authentication needs of institutions for their own systems. The concepts and recommendations discussed here apply to both the institution's needs and services it may provide to customers. However, additional controls not discussed here are needed when certificate authority services are provided to others.

A properly implemented and maintained PKI may provide a strong means of customer identification over open networks such as the Internet. By combining a variety of hardware components, system software, policies, practices, and standards, PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality. The system is based on public key cryptography in which each customer has a key pair-- a unique electronic value called a *public key* and a mathematically related *private key*. The *public key* is made available to those who need to verify the customer's identity. The *private key* is stored on the customer's computer or a separate device such as a smart card. When the key pair is created with strong encryption algorithms and input variables, the probability of deriving the private key from the public key is extremely remote. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure. The private key is used to create an electronic identifier called a *digital signature* that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

The *certificate authority* (CA), which may be the financial institution or its service provider, plays a key role by attesting with a *digital certificate* that a particular public key and the corresponding private key belongs to a specific individual or system. It is important when issuing a digital certificate that the registration process for initially verifying the identity of customers is adequately controlled. The CA attests to the individual's identity by signing the digital certificate with its own private key, known as the *root key*. Each time the customer establishes a communication link with the financial institution, a digital signature is transmitted with a digital certificate. These electronic credentials enable the institution to determine that the digital certificate is valid, identify the individual as a customer, and confirm that transactions entered into the institution's computer system were performed by that customer.

The customer's private key exists electronically and is susceptible to being copied over a network as easily as any other electronic file. If it is lost or compromised, the customer can no longer be assured that messages will remain private or that fraudulent or erroneous transactions would not be performed. Customer agreements and education should emphasize the importance of safeguarding a private key and promptly reporting its compromise.

Although PKI is not widely used for retail-based electronic banking systems, it is an emerging tool, particularly in the commercial sector. PKI minimizes many of the vulnerabilities associated with passwords because it does not rely on shared secrets to authenticate customers, and its electronic credentials are difficult to compromise. The primary drawback of a PKI authentication system is that it is more complicated and costly to implement than user names and passwords. Whether the financial institution acts as its own CA or relies on a third party, the institution should ensure its certificate issuance and revocation policies and other controls discussed below are followed.

When utilizing PKI policies and controls, financial institutions need to consider the following:

- Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure-- expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;

- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a customer's private key or the closure of customer accounts;
- Updating the database of revoked certificates frequently, ideally in real time mode;
- Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;
- Requiring regular independent audits to ensure controls are in place, public and private key lengths remains appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

Tokens

The use of a token represents authentication using "something the customer possesses." Typically, a token is part of a two-factor authentication process, complemented by a password as the other factor. There are many benefits to the use of tokens. The authentication process cannot be completed unless the device is present. Static passwords or biometric identifiers used to activate the token may be authenticated locally by the device itself. This process avoids the transmission of shared secrets over an open network such as the Internet.

Physical devices designed for use in authentication systems have different capabilities. Some are designed only to hold authenticating information, while others are capable of processing information obtained from a database. Various physical objects such as rings, key chains, watches, telephones, or credit and debit cards may contain chips that generate passwords, hold customer credentials, or process information when brought into contact with computers, card readers, or other such "receivers." Tokens utilizing the chip technology embedded in cards are known as *smart cards*.

Password generating tokens provide an effective defense against password guessing because the token generates a new password at specified intervals or provides a unique password in response to a challenge message sent by the institution. In addition, these tokens are easy to use and relatively inexpensive. Password-generating tokens are used by a number of financial institutions to authenticate commercial customers seeking to remotely access the institution's electronic banking system. As costs decrease further, financial institutions may choose to provide retail customers with such tokens.

PKI systems can incorporate tokens or smart cards that contain credentials. For additional security, a financial institution may require that a customer's digital certificate be stored on a smart card. Smart cards and other consumer devices containing electronic chips may be more

costly than software solutions. However, storing private keys on a token instead of on a computer's hard drive prevents unauthorized parties from accessing the user's computer and copying encryption keys without the user's knowledge.

When utilizing tokens, financial institutions need to consider the following:

- Educating customers to ensure they understand their responsibility to safeguard tokens or smart cards, including agreements and rules on their use, protection, and replacement;
- Designing and implementing a secure process for generating and distributing tokens, including agreements and rules on their use, protection and replacement;
- Ensuring that two-factor authentication processes that use tokens limit the number of login attempts that a customer can make in the authentication process; and
- Determining an appropriate expiration date and renewal and revocation processes for customer held tokens.

Biometrics

A biometric identifier measures an individual's unique physical characteristic or behavior and compares it to a stored digital template to authenticate that individual. A biometric identifier representing "something the user is" can be created from sources such as a customer's voice, fingerprints, hand or face geometry, the iris or retina in an eye, or the way a customer signs a document or enters keyboard strokes. The success of a biometric identifier rests on the ability of the digitally stored characteristic to relate typically to only one individual in a defined population. Although not yet in widespread use by financial institutions for authenticating existing customers, biometric identifiers are being used in some cases for physical access control.

Financial institutions could use a biometric identifier for a single or multi-factor authentication process. ATMs that implement iris-scan technologies are an example of the use of a biometric identifier to authenticate users. The biometric identifier may replace the PIN. A customer can supply a PIN or password to supplement the biometric identifier, making it part of a more secure two-factor authentication process. Financial institutions may also use biometric identifiers for automating existing processes, thereby reducing costs. For example, a financial institution may allow a customer to reset a password over the telephone with voice-recognition software that authenticates the customer.

An authentication process that relies on a single biometric identifier may not work for everyone in a financial institution's customer base. Introducing a biometric method of authentication requires physical contact with each customer to initially capture the physical identifier. This process increases deployment costs. Unlike a password or PIN system, in which a financial institution needs to communicate with a customer only once for account initiation, use of biometric identifiers for authentication may require customers to submit several samples, sometimes over time. Some customers may not be able to produce a given biometric identifier, because of particular physical attributes or disabilities.

Even when the customer is able to produce a biometric identifier, there may be times when the biometric identifier cannot authenticate the customer. For example, if a customer has a severe cold, or laryngitis, voice recognition identifiers may mistakenly restrict the customer's access. Financial institutions can eliminate this problem by allowing for more variation in the biometric

sample input compared to the database, but this will reduce overall security and potentially increase the number of individuals that the system may falsely authenticate.

Financial institutions should consider privacy concerns when using biometric identifiers. For example, some customers may associate fingerprint-based biometric identifiers with law enforcement.

When utilizing biometric identifiers, financial institutions need to consider the following:

- Designing systems that encrypt biometric identifiers during storage or transmission;
- Designing and implementing a secure process for capturing biometric identifiers; and
- Limiting the number of failed logons a customer can attempt.