NIST Special Publication 800-63

DRAFT Recommendation for Electronic Authentication

William E. Burr
W. Timothy Polk
Donna F. Dodson

NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

NIST Special Publication 800-63

Recommendation for Electronic Authentication

William E. Burr
W. Timothy Polk
Donna F. Dodson
Computer Security Division
Information Technology Laboratory

January 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

National Institute of Standards and Technology Special Publication 800-63
Natl. Inst. Stand. Technol. Spec. Publ. 800-63, XXpages (January 2004)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Abstract

This recommendation provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

KEY WORDS: Authentication; Authentication Assurance, Credentials Service Provider, Cryptography, Electronic Authentication, Electronic Credentials, Electronic Transactions, Electronic Government, Identity Proofing, Passwords, PKI, Public Key Infrastructure, Tokens.

Executive Summary

E-authentication is the remote authentication of individual people over a network, for the purpose of electronic government and commerce. This recommendation provides technical guidance to agencies in the implementation of electronic authentication to allow an individual person to remotely authenticate his/her identity to a Federal IT system.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum meets the technical requirements for the required level of assurance. In particular, the document states specific technical requirements for each of the four levels of assurance in the following areas:

- Identity proofing and registration including the delivery of credentials
- Tokens for proving identity
- Remote authentication mechanisms
- Assertion mechanisms

A summary of the technical requirements for each of the four levels is provided below.

Level 1 - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3 or 4, including PINS. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange will be able to find the password with a straightforward dictionary attack. Therefore there is not a requirement at this level to use FIPS approved cryptographic techniques.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Session tokens issued to claimants as a result of a successful authentication are either cryptographically authenticated by relying parties, (using FIP approved methods) or are obtained from directly from the verifier via an authenticated protocol that meets Level 3 or Level 4.

Level 2 - A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented. FIPS approved cryptography is required.

Level 3- Level 3 authentication is based on proof of possession of a key or password through a cryptographic protocol. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. Three kinds of tokens may be used: cryptographic (soft and hard) tokens, one-time password device tokens, and password tokens used in zero knowledge password protocols.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and CSP, however session (temporary) shared secrets may be provided to verifiers by the CSP. FIPS approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process. As required, data may also optionally be encrypted under keys derived in the authentication process (note: encryption does not guarantee authentication). Relying parties must determine which data requires authentication or confidentiality protection, and are not required to authenticate or encrypt all data transferred.

Level 4 - Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that “hard” cryptographic tokens are required. The token is a hardware cryptographic module validated at FIPS 140-2 Level 2 or above. By requiring a physical token, which cannot readily be copied and which must be unlocked with a password or biometric, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or relying parties by the CSP. Strong, FIPS approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys derived in the authentication process.

Table of Contents

1 Purpose

This recommendation provides technical guidance to agencies in the implementation of electronic authentication (e-authentication).

2 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

3 Introduction

E-authentication is the remote authentication of individual people over a network, for the purpose of electronic government and commerce. In e-authentication, an individual person remotely authenticates his or her identity to a Federal IT system.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] that defines four levels of assurance Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The guidance defines required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

This document states specific technical requirements for each of the four levels of assurance in the following areas:

- Identity proofing, registration and the delivery of credentials,
- Tokens for proving identity,
- Remote authentication mechanisms, that is the credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,
- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

This technical guidance covers remote electronic authentication of human users of Federal agency IT systems over a public network. It does not address the authentication of a person who is physically present, for example for access to buildings, although some credentials and tokens that are used remotely may also be used for local authentication. While this technical guidance does, in many cases, establish requirements that Federal IT systems and service providers participating in authentication protocols be authenticated to subscribers, it does not specifically address machine-to-machine (such as router-to-router) authentication, nor does this guidance establish specific requirements for issuing authentication credentials and tokens to machines and servers when they are used in e-authentication protocols with people.

The paradigm of this document is that individuals are enrolled and undergo an identity proofing process. Thereafter, they are remotely authenticated to systems and applications over an open network. The document covers only authentication mechanisms that work by making the individual demonstrate possession and control of a secret. It may also be practical to achieve authentication by testing the personal knowledge of the individual (referred to as knowledge based authentication.) This recommendation does not consider such authentication methods; however, NIST is studying this subject and plans to issue guidance on it. When developing e-authentication solutions agencies should consult *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* [OMB 03-22].

4 Definitions and Abbreviations

Active Attack	An attack on the authentication protocol where the attacker transmits data to the claimant or verifier (ex. impersonation, man-in-the middle attack, session hijacking).
Attack	An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token.
Attacker	A party who is not the claimant or verifier but wishes to successfully execute the authentication protocol as a claimant.
Approved	FIPS approved or NIST recommended: an algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation.
Assertion	A statement from a verifier to a relying party that contains identity or attribute information about a subscriber.
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, for example encryption and decryption or signature generation and signature verification.
Authentication Protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authenticity	The property that data originated from its purported source.
Bit	A binary digit: 0 or 1.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and signed by a Certification Authority. See [RFC 3280]
Challenge-response protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the verifier combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, the password itself is not directly intercepted by an eavesdropper, but the eavesdropper may be able to find the password with an off-line passwords guessing attack.
Claimant	A party whose identity is to be verified using an authentication protocol.

Credentials Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may include a Registration Authority (RA).
Cryptographic key	A randomly generated secret value used in a cryptographic algorithm. For the purposes of this document, keys must contain at least 80-bits of entropy. This means that it must be as hard to find the key, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number.
Cryptographic strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined to mean that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion, that is it requires at least on the order of 2^{79} operations.
Cryptographic token	A token where the secret is a cryptographic key.
Data Integrity	The property that data has not been altered by an unauthorized entity.
Digital Signature	An asymmetric key operation where the private key is used to sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. See Appendix A.
FIPS	Federal Information Processing Standard.
HMAC	Hashed-based Message Authentication Code: a symmetric key authentication method using hash functions.
Identity	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique.
Identity Proofing	The process by which a CSP and an RA validate sufficient information to uniquely identify a person.
Kerberos	A widely used authentication protocol developed at MIT. In "classic" Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a "ticket" by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user to a KDC exchange.
Man-in-the-middle attack	An attack on the authentication protocol run in which the attacker positions himself in between the claimant and verifier so that he can intercept and alter data traveling between them.

Message Authentication Code (MAC)	A cryptographic checksum on data that is designed to reveal both accidental and intentional modifications of the data.
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Off-line attack	An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.
On-line attack	An attack against an authentication protocol where the attacker poses as a subscriber, acts as a claimant to a verifier and attempts to gain authenticated access or learn authentication secrets.
On-Line Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
Passive attack	An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping).
Password	A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Private key	The secret part of an asymmetric key pair that is typically used to sign or decrypt data.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a key or password.
Public key certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. See [RFC 3280]
Public key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Registration Authority (RA)	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Salt	A non-secret value that is used in cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.
Security Assertion Markup Language (SAML)	A specification for encoding security assertions in the XML markup language. See: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
Shared secret	A secret used in authentication that is known to the claimant and the verifier.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Symmetric key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Transport Layer Security (TLS)	An authentication and security protocol implemented in current browsers and web servers. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1.
Tunneled password protocol	A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier public key certificate to authenticate the verifier to the claimant and establish an encrypted session between the verifier and claimant. The encrypted TLS session then protects the claimant's password from eavesdroppers.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.
Verifier impersonation attack	An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password.
Zero knowledge password authentication protocol	An authentication protocol in which the claimant and verifier learn nothing about the password as a result of a protocol run that they didn't already know before the run.

5 E-Authentication Model

In this guidance, the individual claiming an identity is called a *claimant* and the party verifying that identity is called a *verifier*. E-authentication begins with *registration*. Before an individual can claim an identity, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called *identity proofing*, and, in the lexicon of this guidance, identity proofing is performed by a *Registration Authority (RA)*, a trusted entity that registers individual *subscribers* with a *Credentials Service Provider (CSP)*. The CSP registers or gives the subscriber a *token* to be used in an authentication protocol and issues *credentials* as needed to bind that token to the identity, or to bind the identity to some other useful attribute. When a *claimant* successfully demonstrates possession and control of a token in an on-line authentication to a *verifier* through an *authentication protocol*, the verifier can establish the identity of the subscriber. A verifier can pass along an assertion about the identity or provide an attribute of the claimant to a *relying party*. The relying party can used the authenticated identity and other factors to make access control or authorization decisions.

Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has; this is a separate decision. *Relying parties*, typically government agencies, who rely on the authenticated identity of a party, will use that authenticated identity and other factors to make access control or authorization decisions. In many cases, the authentication process and services will be shared by many applications and agencies, but the individual agency or application is the relying party that must make the decision to grant access or process a transaction based on the specific application requirements. This guidance provides technical recommendations for the process of authentication, not authorization.

5.1 Subscriber, RA and CSP

In the conceptual e-authentication model, a claimant in an authentication protocol must be a subscriber to some CSP. At some point, the subscriber registers with an RA, which verifies the identity of the subscriber, typically through the presentation of paper credentials and by records in databases. This process is called identity proofing. The RA, in turn, vouches for the identity of the subscriber to a CSP. The CSP registers or gives the subscriber a token to be used in an authentication protocol and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful attribute. The subscriber may be given electronic credentials to go with the token at the time of registration, or credentials may be generated later as needed.

There is always a relationship between the RA and CSP. In the simplest and perhaps the commonest case, the RA/CSP are separate functions of the same entity. However, an RA might be part of a company or organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have relationships with different CSPs as well.

Section 7 provides recommendations for the identity proofing and registration process.

5.2 Tokens

Tokens are something that the claimant possesses and controls that may be used to authenticate the claimant's identity. In e-authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for e-authentication shall include some secret information and it is important to provide security for the token. In fact, the three factors often considered as the cornerstone of authentication:

- Something you know (for example, a password)
- Something you have (for example, a cryptographic key or smart card)
- Something you are (for example, a voice print or other biometric)

influence the security provided by tokens. Tokens that incorporate all three factors are stronger than tokens that only incorporate one or two of the factors.

The secrets are often based on either *public key pairs* or *shared secrets*. *Public keys* are one half of a public key pair (also known as an asymmetric key), and the other half, a related *private key*, is used as a token. A verifier, knowing a claimant's public key through some credential (typically a *public key certificate*), can use an authentication protocol to verify the claimant's identity, by proving that the claimant has control of the associated private key token (*proof of possession*).

Shared secrets are either *symmetric keys* or passwords. In a protocol sense, all shared secrets are similar, and can be used in similar authentication protocols; however, passwords, since they are often committed to memory, are something the claimant knows, rather than something he has. Passwords, because they are committed to memory, usually do not have as many possible values as cryptographic keys, and, in many protocols, are vulnerable to network attacks that are impractical for keys. Moreover the entry of passwords into systems (usually through a keyboard) presents the opportunity for very simple keyboard logging or "shoulder surfing" attacks. Therefore keys and passwords demonstrate somewhat separate authentication properties (something you know rather than something you have) and passwords often have lesser resistance to network attacks. However, when using either public key pairs or shared secrets, the subscriber has a duty to maintain exclusive control of his token, since possession or control of the token is used to authenticate the subscriber's identity.

Biometrics are unique personal attributes that can be used to identify a person. They include facial pictures, fingerprints, DNA, iris and retina scans, voiceprints and many other things. The view of this guidance is that biometrics values should not be considered secrets in authentication processes, since the biometrics can often be observed, and since they are innate to the person and cannot be changed. Since they are not secrets, biometrics cannot serve as tokens for e-authentication. Therefore biometrics by themselves are of limited value in the remote e-authentication processes that are the subject of this guidance. Biometrics are valuable where the claimant is physically present at a reader controlled by the verifier, in registration processes to be able to later prove who actually registered and received credentials, and, in some cases, to unlock the keys of hardware tokens.

As defined in Section 6, this guidance recognizes four kinds of claimant tokens: hard tokens, soft tokens, one-time password device tokens and password tokens.

5.3 Electronic Credentials

Paper credentials are documents that attest to the identity or other attributes of an individual or entity called the subject of the credentials. Some common paper credentials include passports, birth certificates, driver's licenses, and employee identity cards. The credentials themselves are authenticated in a variety of ways: traditionally perhaps by a signature or a seal, special papers and inks, high quality engraving, and today by more complex mechanisms, such as holograms, that make the credentials recognizable and difficult to copy or forge. In some cases, simple possession of the credentials is sufficient to establish that the physical holder of the credential is indeed the subject of the credentials. More commonly, the credentials contain biometric information such as the subject's description, a picture of the subject or the handwritten signature of the subject that can be used to authenticate that the holder of the credentials is indeed the subject of the credentials. When these paper credentials are presented in-person, authentication biometrics contained in those credentials can be checked to confirm that the physical holder of the credential is the subject.

Electronic identity credentials bind an identity and perhaps other attributes to a token. This recommendation does not prescribe particular kinds of electronic credentials. There are a variety of electronic credential types in use today, and new types of credentials are constantly being created. Electronic credentials may be general purpose credentials or targeted to a particular verifier. Some common types of credentials are:

- X.509 public key identity certificates bind an identity to a public key;
- X.509 attribute certificates that bind an identity or a public key with some attribute;
- Kerberos tickets that are encrypted messages binding the holder with some attribute or privilege.

Electronic credentials may be stored as directory objects. These credentials may be signed objects (e.g., X.509 certificates), in which case they are self-authenticating. In this case, the directory may be an untrusted entity. Alternatively, the directory may be a trusted entity. When the directory is trusted, credentials may simply be stored as a directory entry.

5.4 Verifiers

In any authenticated on-line transaction, the verifier must verify that the claimant has possession and control of the token that verifies his or her identity. A claimant authenticates his or her identity to a verifier by the use of a token and an authentication protocol. This is called *Proof of Possession (PoP)*. Many PoP protocols are designed so that a verifier, who has no knowledge of the token before the authentication protocol run, learns nothing about the token from the run. It is undesirable for verifiers to learn shared secrets unless they are also the CSP who registered the tokens. The verifier and CSP may be the same entity, the verifier and relying party may be the same entity or they may all three be separate entities. Where the verifier and the relying party are separate entities, the verifier must convey the result of the authentication protocol to the relying party. The object created by the verifier to convey this result is called an assertion.

5.5 Assertions

Assertions can be used to pass information about the claimant or the e-authentication process from the verifier to a relying party. Assertions support the claimant's identity but are not bound to the token possessed by the claimant. A relying party trusts an assertion based on the source, the time of creation, and attributes associated with the claimant.

Examples of assertions include:

- SAML assertions, specified using a mark up language intended for describing security assertions, can be used by a verifier to make a statement to a relying party about the identity of a claimant.
- Cookies, character strings placed in a web browser's memory, are available to websites with the same domain name as the entity that placed them in the web browser. Cookies may simply be tickets or may contain pointers to verified credentials.[1]

Assertions may be stored as directory objects. Where assertions are signed objects (e.g., signed SAML assertions), they are self-authenticating. Alternatively, the directory may be a trusted entity. When the directory is trusted, unsigned assertions may be accepted based on the source.

5.6 The Relying Party

A relying party relies on results of an on-line authentication to establish the identity or attribute of a subscriber for the purpose of some transaction. The verifier and the relying party may be the same entity, or they may be separate entities. If they are separate entities, the relying party receives an assertion from the verifier. The relying party is responsible to validate that the received assertion came from a verifier trusted by the relying party. Where the assertions indicate time of creation or attributes associated with the claimant, the relying party is also responsible for verifying this information.

[1] There are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

6 Tokens

This guidance recognizes four kinds of claimant tokens for e-authentication. Each type of token incorporates one or more of the factors (something you know, something you have, and something you are.) Tokens that provide a higher level of assurance incorporate two or more of the factors. The four kinds of tokens include:

- *Hard token* – a hardware device that contains a protected cryptographic key. Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall:
  - require the entry of a password or a biometric to activate the authentication key;
  - not be able to export authentication keys;
  - be FIPS 140-2 validated:
    - overall validation at Level 2 or higher,
    - physical security at Level 3 or higher.

- *Soft token* – a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token shall be encrypted under a key derived from a password known only to the user, so knowledge of a password is required to activate the token. The cryptographic module used with the soft token shall be validated at FIPS 140-2 Level 1 or higher. Each authentication shall require entry of the password and the unencrypted copy of the authentication key shall be erased after each authentication.
- *One-time password device token* - a personal hardware device that generates "one time" passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by using a FIPS approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, or a counter generated on the device, or a challenge sent from the verifier (if the device has an entry capability). The device shall be validated at FIPS 140-2 Level 1 or higher. The one-time password typically is displayed on the device and manually input (direct electronic input from the device to a computer is also allowed) to the verifier and as a password.
- *Password token* – a secret character string that a claimant memorizes and uses to authenticate his or her identity.

Impersonation of an identity using a hard or soft token requires that the impersonator obtain two separate things: either the key (token) and a password, or the token and the ability to enter a biometric into the token. Therefore both hard and soft tokens provide more assurance than passwords by themselves normally provide. Moreover, a hard token is a physical object and its theft is likely to be noticed by its owner, while a soft token can sometimes be copied without the owner being aware. Therefore a hard token offers more assurance than a soft token.

Impersonation of an identity using a password token requires only that the impersonator obtain the password. The ability of humans to remember long, arbitrary passwords is limited, so password tokens are often vulnerable to a variety of attacks including guessing, dictionaries of commonly used passwords, and simple exhaustion of all possibilities. There are a wide variety of password authentication protocols that differ significantly in their vulnerabilities, and many password mechanisms are vulnerable to passive and active network attacks. While some cryptographic password protocols resist nearly all direct network attacks, these techniques are not at present widely used and all password authentication mechanisms are vulnerable to keyboard loggers and observation of the password when it is entered. Therefore password tokens generally provide less assurance than hard or soft tokens.

7 Identity Proofing and Registration

Identity proofing is the process of ensuring that an identity is actually a real person, with correctly associated attributes (perhaps only a name). Increasing levels of assurance require increasing effort to establish the identity of subscribers.

In this document, an entity that does identity proofing is a Registration Authority (RA). This term is taken from common PKI usage, but in this document, an RA may register, that is verify the identity of subscribers for other technical mechanisms such as passwords, as well as for PKI. This guidance does not prescribe the relationship between an RA and a CSP. The RA may be subordinate to or an integral part of the CSP or it may be entirely independent of the CSP, although some relationship must exist between the two. For example, the RA may be a part of a public CSP. An individual, wishing to be issued identity credentials applies to the RA component of the CSP, and is issued credentials and tokens. An RA could also be associated with a company or other organization and verify the identity of that organization's employees or members to an independent CSP. That independent CSP might have a business relationship with many organizations and their RAs.

7.1 Identity Proofing and Registration Threats

There are general attacks that can occur during the identity proofing and registration process where an attacker attempts to claim an identity of another individual in such a way that the CSP will provide an improper credential to the attacker.

7.1.1 Identity Proofing and Registration Threat Model

One way to categorize registration process attacks is to look at the level of effort required to obtain a credential in another person's name, or in the name of a fictitious person. These attacks may be classified as *targeted* or *untargeted* attacks. In a targeted attack, the attacker wishes to impersonate a specific individual. In untargeted attacks, the attacker wishes to create a subscriber relationship with the CSP, but does not care which individual is associated with the credential. The attacker is often attempting to impersonate any individual to create a subscriber relationship with the CSP.

Specific attacks that can occur during the identity proofing and registration process include:

- Impersonation – A claimant masquerades as a selected real individual with the goal of obtaining credentials in that individual's name.
    - Casual Impersonation – The attacker supports the claimed identity using information obtained from publicly available sources (e.g., information obtained from Internet searches).

- Systematic Impersonation – The attacker supports the claimed identity using false paper credentials with the name and address of the real person combined with the attacker's biometric. For example, the attacker may obtain a fake driver's license with his/her photograph and the subscriber's name and address.

- Impersonation through Physical Access – The attacker supports the claimed identity by demonstrating physical access to the real subscriber's home or workplace to support their claim of identity (e.g., by receiving mail or placing a phone call from an address of record).

- Insider Impersonation – The attacker supports the claimed identity of the subscriber using his/her knowledge of information that would not be generally available from public sources. (This attacker is assumed to also have physical access.)

- Fictitious Subscriber – An attacker claims the identity of a non-existent person with the goal of obtaining subscriber credentials with that identity.[2] For example, the attacker acts as a subscriber and supports his/her false identity with valid-sounding data (e.g., fake address, etc.).

- Rogue Infrastructure Component – A CSP or RA uses their trusted position to create or obtain credentials, allowing the CSP or RA to masquerade as either a potential subscriber or a non-existent person.

  - Falsification of Registration Data - The attacker is an RA who creates and authenticates a false request from a real or imaginary person to obtain credentials in that subscriber's name.

  - Unrequested Credential – The attacker is the CSP, who creates a credential without a corresponding request from a subscriber or RA.

7.1.2 Resistance to Registration Fraud Threats

Resistance to registration fraud can be achieved by precluding certain classes of attacks and increasing the cost and effort involved in others. This section identifies mechanisms for increasing resistance to the threats identified in the previous section. Resistance to registration fraud is increased either by making a successful impersonation more difficult, or by deterring would-be impersonators by increasing the risks that they run.

- *Impersonation Resistance* - The RA can employ various mechanisms to detect or resist an attacker who has claimed another person's identity. Techniques include verification of the applicant's:

  - *Knowledge of static personal facts*, such as the date and place of birth or mother's maiden name, pertaining to the claimed identity. Verification of knowledge of

[2] Note that we do not consider the case where a subscriber that has obtained legitimate paper credentials for a fictitious person. This was judged out of scope.

static facts or information that rarely changes, such as addresses, provides resistance to targeted attacks by casual impersonators.

- *Dynamic personal facts*, such as the current balance of a bank account, the amount of a previous utility bill, or actual use of a credit card (because credit card is continuously monitored). Verification of these rapidly changing facts provides resistance to targeted and untargeted attacks by casual impersonators.

- *Physical access* to the home, office or telephone associated with the claimed identity (e.g., by retrieving mail, placing or receiving a phone call, etc.). This mechanism provides resistance to target and untargeted casual and systematic impersonation attacks.

- *Possession of supporting paper credentials presented to the RA*, who reviews the data and any biometrics (e.g., photographs) on the supporting credentials. This in-person proofing mechanism provides resistance to some systematic impersonation attacks, as poor quality fraudulent supporting paper credentials may be identified by the RA

- *Possession of verifiable supporting paper-based credentials,* that the RA verifies the validity of with the credential issuer, so that the RA confirms that paper-based credentials were truly issued, have not been not been revoked, and the facts stated in the credentials are consistent with the records of the issuer. This provides resistance to most systematic impersonation attacks.

- *Fictitious Identity Detection* - The RA or CA can employ various mechanisms to detect an attacker who attempts to create a fictitious identity. Techniques include verification of:

  - *Applicant existence in databases* that contain historical information, such as credit databases

  - *Presentation of supporting paper credentials* to ensure that the credentials are valid and were actually issued by their issuer.

- *Registration Fraud Deterrence* – Registration fraud of all types can be deterred by recording the applicant's biometric (e.g. a photo) during the registration process. This does not make it harder for the applicant to commit fraud, but it does make it much more risky, and prevents legitimate applicants from disavowing their registration. It is particularly effective at deterring insider impersonation, since the victim will usually be able to identify the impersonator.

- *Rogue Infrastructure Component Resistance* – Policy and procedural controls can be established and maintained to detect or prevent improper actions by a Rogue RA or CSP.

  - *Pre-approved Credentials*. In this case, the CSP will not issue credentials unless the subscriber has been pre-approved. This provides resistance against falsified registration data attacks by a Rogue RA

- *Audit trail establishment and control.* The CSP and RA may be required to compile and maintain audit records. This provides resistance against falsified registration data attacks and unrequested credential attacks by a Rogue RA, as the lack of supporting evidence will point to RA malfeasance. Similarly, this provides resistance to unrequested credential attacks by the CSP, since the audit trail will not contain the corresponding request from the RA.

7.2 Identity Proofing and Registration Process Levels

The following sections list the NIST recommendations for registration and identity proofing for the four levels corresponding to the OMB guidance. As noted in the OMB guidance, Levels 1 and 2 recognize the use of anonymous credentials. When anonymous credentials are used to imply membership in a group, the level of proofing should be consistent with the requirements for the identity credential of that level. Explicit requirements for registration processes for anonymous credentials are not specified as they are unique to the membership criteria for each specific group.

At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on their relationship. Either the RA or the CSP shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his/her identity, including the evidence required in the sections below. The identity proofing and registration process shall be performed according to a written policy or *practice statement* that specifies the particular steps taken to verify identities. When PKI is employed by the CSPs and RAs, this information is usually contained in the *Certificate Policy* or *Certification Practice Statement* of the CA. Therefore a separate registration policy or practice statement need not be created if it is covered in either of these documents.

7.2.1 Level 1

There is no requirement to prove the identity or maintain a record of the facts of registration at this level. Identity assertions of claimants are accepted without verification.

7.2.2 Level 2

Level 2 identity proofing and registration provides sufficient assurance for relatively low-risk, routine business transactions. In many cases it can be accomplished on-line and immediately. To conform to Level 2, RAs/CSPs shall meet the requirements found in section 7.2.2.1 General Requirements with the exception of Public Key Certification Authorities that have cross-certified with the Federal Bridge CA. The requirements for CAs that have cross-certified with the Federal Bridge CA are stated in 7.2.2.2.

7.2.2.1 General Requirements

These identity proofing and registration requirements apply at Level 2 for RAs and CSPs. The RA shall ensure that the applicant's identity information is verified and checked in accordance with the stated registration policy. Identity information shall include at a minimum, full legal name and other supporting verifiable information sufficient to uniquely identify the applicant. A record of the facts of registration shall be maintained by the CSP or its representative. The

minimum record retention period for registration data for Level 2 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs operated by or on behalf of executive branch agencies must also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

If the RA and CSP are remotely located, and communicate over a network, the communications including the entire registration transaction between RA and CSP shall be cryptographically protected with an approved method such as TLS and an authentication mechanism that meets the requirements for at least Level 2 assurance.

The RA/CSP may be a government organization, corporation, or other organization issuing credentials to individuals with whom it has an ongoing relationship (e.g., employee, customer, affiliate or member), or it may be a public CSP issuing credentials to individuals with whom it has no prior or independent relationship.

7.2.2.1.1 Organizational RA/CSP

This section applies to the registration of applicants who have a significant, established on-going relationship (e.g., employee, customer, financial institute client, member) with an organization (e.g., business, financial institution, government agency, professional society) and the organization operates a recognized RA or CSP. The relationship must rely upon the identity of the applicant and include a duty or strong financial reason to know the identity of the applicant for significant purposes such as:

- employment
- government program client
- banking
- extension of credit of $2,000 or more
- issuance of insurance
- regular payment of bills and a duty of the organization to know the true identity of the applicant
- matriculation at an accredited degree granting educational institution
- compliance with public safety, health or other government regulations that impose a duty to verify the identity or members or participants.

At a minimum, the registration process shall:

1) Confirm that the claimed identity of the applicant is a person with an authenticated ongoing business relationship to the organization.
2) Issue or renew credentials and tokens in a manner that binds the verified identity with the confirmed:
    a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record), or
    b) telephone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record), or

c) e-mail or other electronic business communications address of record (for example, by sending an authenticator to the applicant's e-mail address.)

7.2.2.1.2 Public RA/CSP

This section applies to the registration of applicants by recognized RAs/CSPs that serve the public at large. The ID proofing process may be either in-person or remote.

7.2.2.1.2.1 Remote Registration

Remote registration can take place over the Internet, by postal mail or by telephone. At a minimum the registration process shall:

1) Verify the details of the claimed identity through either:
   a) credit records or similar databases that the claimed identity exists and is consistent with identity and address information provided by the applicant; or
   b) the presentation of a valid credit or non-prepaid bank card number, using an address of record for the card number which is consistent with the address information provided by the applicant.
2) Issue or renew credentials and tokens in a manner that binds the verified identity with the confirmed:
   a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record); or
   b) telephone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record); or
   c) e-mail or other electronic business communications address of record (for example, by sending an authenticator to the applicant's e-mail address.)

7.2.2.1.2.2 In-person Registration

In-person registration requires that the applicant present himself in-person to the RA with paper identity credentials. At a minimum, the registration process shall:

1) Establish the applicant's identity by presenting to the Registration Authority a current government issued primary photo-ID, such as a driver's license, military ID or passport.
2) Issue or renew credentials and tokens in a manner that binds the verified identity with the confirmed:
   a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record);or
   b) telephone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record); or
   c) e-mail or other electronic address of record (for example, by sending an authenticator to the applicant's e-mail address.)

7.2.2.2 FPKI Managed Certificates

The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Basic, Citizen and Commerce Class, Medium, High or Common Certificate Policy [BASIC, CITIZ, MED, HIGH, COMM] levels are deemed to meet the identity proofing provisions of Level 2. However, agencies are

not limited to relying upon only those certificates by CAs cross-certified with the Federal Bridge CA. At Level 2, agencies may choose to rely on any CA that has been determined to meet the identity proofing and registration requirements stated in the General Requirements, Section 7.2.2.1.

7.2.3 Level 3

Level 3 identity proofing requires that RAs verify substantial evidence of the identity of applicants; however, it does not necessarily require that applicants present themselves in person to register. Level 3 identity proofing generally requires that the current status of at least some of the credentials or records used to validate an identity be confirmed as valid and current. It also requires confirmation of a physical address or phone number of record. To conform to Level 3, RAs/CSPs shall meet the requirements found in section 7.2.3.1 General Requirements with the exception of Public Key Certification Authorities. The requirements for CAs are stated in 7.2.3.2.

7.2.3.1 General Requirements

These identity proofing and registration requirements apply at Level 3 for RAs and CSPs. The RA shall ensure that the applicant's identity information is verified and checked in accordance with the stated registration policy. Identity information shall include at a minimum:

- Full legal name
- Date and place of birth (may not be verified but should be collected)
- Current address of record
- The identity numbers of any documents checked in the registration process, such as passport number, social security number, driver's license number, etc.

A record of the facts of registration, including the steps taken and copies of any documents examined to verify the subscriber's identity, shall be maintained by the CSP or its representative. The minimum record retention periods for registration data for Level 3 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs operated by or on behalf of executive branch agencies must also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

If the RA and CSP are remotely located, and communicate over a network, the entire registration transaction shall be cryptographically authenticated using an authentication protocol that meets the requirements for Level 3 or higher and encrypted using an approved encryption method.

The RA/CSP may be a government organization, corporation, or other organization issuing credentials to individuals with whom it has an ongoing relationship (e.g., employee, customer, affiliate or member), or it may be a public CSP issuing credentials to individuals with whom it has no prior or independent relationship.

7.2.3.1.1 Organizational RA/CSP

This section applies to the registration of applicants who have established a significant on-going relationship (e.g., employee, customer, financial institute client, member) of one year or longer with an organization (e.g., business, financial institution, government agency, professional society) and the organization operates a recognized RA or CSP. The relationship shall rely upon the identity of the applicant and include a duty to know the identity of the applicant for significant purposes such as:

- employment
- government program client
- banking
- extension of credit of $2000 or more
- issuance of insurance
- regular payment of bills and a duty of the organization to know the true identity of the applicant
- matriculation at an accredited degree granting educational institution
- compliance with public safety, health or other government regulations that impose a duty to verify the identity of members or participants.

At a minimum the registration process shall:

1) Confirm that the claimed identity of the applicant is a person with a current relationship to the organization of at least one year, and that relationship is in good standing.
2) Issue or renew credentials and tokens in a manner that binds the verified identity with the confirmed:
    a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record); or
    b) phone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record).

7.2.3.1.2 Public RA/CSP

This section applies to the registration of applicants by recognized RA/CSPs who do not yet have a significant established on-going relationship with the applicant of at least one year or longer. The ID proofing process may be either in-person or remote:

7.2.3.1.2.1 Remote Registration:

Remote registration can take place electronically or by mail. At a minimum the registration process shall:

1) Verify the details of the claimed identity through:
    a) credit cards or similar databases that the claimed identity exists and is consistent with the identity and address information provided by the applicant; and
    b) a currently valid credit or bank card.
2) Issue or renew credentials and tokens in a manner that confirms either:

a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record); or
b) phone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record).

7.2.3.1.2.2 In-person Registration

In-person registration requires that the applicant present himself in-person to the RA with paper identity credentials. At a minimum, the registration process shall:

1) Establish the applicant's identity by in-person proofing before the Registration Authority, based on one of the following sets of identifying materials:
    a) A current government issued primary photo-ID, such as a driver's license, military ID or passport, that is verified to be valid by a records check; or
    b) A current government issued primary photo-ID such as a driver's license, military ID or a passport (no records check) plus at least one of the following:
        - a credit or bank card that is verified to be currently valid; or
        - a current credit check to a recognized resource that confirms the information on the primary photo-ID; or
        - a student ID that is verified to be current and valid.
2) Issue or renew credentials and tokens in a manner that binds the verified identity with the confirmed:
    a) postal address of record of the applicant (for example, by mailing an authenticator to the address of record); or
    b) phone number of the applicant (for example, by requiring a call from or to the applicant's telephone number of record).

7.2.3.2 FPKI Managed Certificates

The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Basic, Citizen and Commerce Class, Medium, High or Common Certificate Policy [BASIC, CITIZ, MED, HIGH, COMM] levels are deemed to meet the identity proofing provisions of Level 3. At this level, PKI credentials shall be issued by a CA cross-certified with the Federal Bridge CA under one of the preceding certificate policies or a policy mapped to one of the preceding policies.

7.2.4 Level 4

Level 4 identity proofing is distinct in that it requires in-person identity proofing of identity documents that contain a picture of the applicant, and that a biometric such as a photograph or fingerprint, be taken of the applicant and retained in the records. The delivery of tokens also shall be linked to the in-person appearance at the RA. This level also requires applicants to sign their application with a handwritten signature under penalty of perjury. To conform to Level 4, RAs/CSPs shall meet the requirements found in section 7.2.4.1 General Requirements with the exception of Public Key Certification Authorities. The requirements for CAs are stated in 7.2.4.2.

7.2.4.1 General Requirements

These identity proofing and registration requirements apply at Level 4 for RAs and CSPs. The RA shall ensure that the applicant's identity information is verified and checked in accordance with the stated registration policy.

A record of the facts of registration, including the steps taken and copies of any documents examined to verify the subscriber's identity, shall be maintained by the CSP or its representative. The minimum record retention periods for registration data for Level 4 credentials is ten years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs operated by or on behalf of executive branch agencies must also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

If the RA and CSP are remotely located, and communicate over a network, the communications between RA and CSP, the entire registration transaction shall be cryptographically authenticated using an authentication protocol that meets the requirements for Level 4 assurance and encrypted using an approved encryption method.

The RA/CSP may be a government organization, corporation, or other organization issuing credentials to individuals with whom it has an ongoing relationship (e.g., employee, customer, affiliate or member), or it may be a public CSP issuing credentials to individuals with whom it has no prior or independent relationship.

Where the RA/CSP issues credentials to employees or Federal affiliates, these procedures require an authenticated request from organization management as the first step. In such cases, the RA/CSP is required to verify one applicant-supplied ID with biometrics. Where the RA/CSP issues credentials to organizational customers, members, or affiliates, two procedural models are defined:

- Where an explicit request from organizational management has been received, the RA/CSP is required to verify one applicant supplied ID with biometrics.

- Where there is no explicit request form from organizational management and therefore compensating verification of additional identity credentials is required.

Public RA/CSPs are required to verify two applicant-supplied credentials.

7.2.4.1.1 Organizational RA/CSP

Corporations or other organizations may be recognized as CSPs for the purpose of issuing credentials and tokens to their employees, customers, members or others with whom they have a close and ongoing relationship.

7.2.4.1.1.1Employees

At a minimum, authentication procedures for employees shall:

1) Verify that a request for credential issuance to the applicant was submitted by organizational management.

2) Verify the applicant's employment through the use of official organizational personnel records.

3) Establish the applicant's identity by in-person proofing before the Registration Authority, based on either of the following processes:

   a) Process #1:

      i) The applicant presents a government-issued form of identification (e.g., a current passport, or driver's license) or an Organization–issued photo I.D. as proof of identity, and

      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

      iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the Organization-issued ID is verified as valid). Typically this is accomplished by querying personnel records maintained by the organization that issued the credential.

   b) Process #2:

      i) The applicant presents a government-issued form of identification (e.g., a current passport, or driver's license) or Organization-issued photo I.D as proof of identity, and

      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

      iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the information (e.g., name and address) on the credential presented in step 3) b) i) above for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA.

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint).

Additionally, the RA shall record the process that was followed for issuance of each credential. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

7.2.4.1.1.2 Customers and Affiliates

For organizational customers, members or other affiliates, two sets of authentication procedures have been defined. Where the organization initiates the request, identity proofing requirements are the same as for employees. Where the customer or affiliate requests the credential, additional requirements are imposed.

Organization-initiated Credential Request

1) Verify that a request for credential issuance to the applicant was submitted by an authorized sponsoring organizational employee;
2) Verify the sponsoring employee's identity and employment through either of the following methods:
    a) A digital signature verified by a currently valid employee signature certificate issued by the CA, may be accepted as proof of both employment and identity, or
    b) Employee's identity shall be established by in-person proofing before the Registration Authority as in employee authentication above and employment validated through use of official organizational records.
3) Establish applicant's identity by in-person proofing before the RA, based on either of the following processes:
    a) Process #1:
        i) The applicant presents a government-issued form of identification (e.g., a passport or driver's license) as proof of identity, and
        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the passport is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential.

b) Process #2:

i) The applicant presents a government-issued form of identification (e.g., a passport or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA.

4) Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA.

The RA shall record the process that was followed for issuance of each credential as described in 7.2.4.1.1.1 above.

Customer-initiated Credential Request

1) Verify that the applicant has an on-going relationship with the organization of at least one year's standing, that involves regular business interaction with the organization, for example regular billing and payment of bills, shipment of goods and performance of services.

2) Establish the identity of applicant by in-person proofing before the organizational RA, based on any of the following sets of identifying materials:

a) two government I.D.s, one of which shall be a photo I.D. (e.g., passport or driver's license); or
b) one government-issued photo I.D. (e.g., passport or driver's license) and one I.D. issued by the organization itself; or
c) one government-issued photo I.D. (e.g., passport or driver's license) and one I.D. issued by a financial or academic institution (e.g., credit card or student identification card); or
d) one government-issued photo I.D. (e.g., passport or driver's license) specifying name and address with a confirming credit report (i.e., a credit report exists for the named person at the given address).

3) Verify that the identity or other information asserted in the credentials and ID documents used to verify identity are consistent with the records of the organization.

4) A biometric of the applicant (e.g., a photograph) shall be recorded.

The RA shall record the process that was followed for issuance of each credential as described in 7.2.4.1.1.1 above.

7.2.4.1.1.2 Public RA/CSP

Recognized CSPs may offer credential-issuing services to the members of the general public, with whom they may have no previous relationship. Authentication procedures shall include the following steps:

1) Establish the identity of applicant by in-person proofing before the RA, based on any of the following sets of identifying materials:

    a) two government I.D.s, one of which shall be a photo I.D. (e.g., passport or driver's license); or
    b) one government-issued photo I.D. (e.g., passport or driver's license) and one I.D. issued by a financial or academic institution (e.g., credit card or student identification card).

2) To ensure legitimacy and consistency, verify all identification information provided by the applicant.

3) Perform a check of credit records or other comparable databases to check for consistency with information supplied by the applicant and stated on identity documents.

4) Record a biometric of the applicant (e.g., a photograph).

The RA shall record the process that was followed for issuance of each credential as described in 7.2.4.1.1.1.

7.2.4.2 FPKI Managed Certificates

The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA at the High or Common Certificate Policy - Hardware [HIGH, COMM] levels are deemed to meet the identity proofing provisions of Level 4. At this level, PKI credentials shall be issued by a CA cross-certified with the Federal Bridge CA under one of the preceding certificate policies or a policy mapped to one of the preceding policies.

7.2.5 Summary of Required Protections by Level

	Level 2			**Level 3**			**Level 4**		
	Org. CSP	Public Remote	Public In-person	Org. CSP	Public Remote	Public In-person	Org. CSP	Org initiated customer cred	Customer initiated
Impersonation Resistance by Verification of:									
Static Facts	√	√	√	√	√	√	√	√	√
Dynamic Facts		√			√	√			
Physical Access	√	√	√	√	√	√			
Possession of Credentials			√			√			
Validity of Credentials							√	√	√ (two credentials)
Fictitious Identity Detection	√	√		√	√		√	√	√
Deterrence: biometric of the applicant							√	√	√
Rogue Infrastructure Component Resistance									
Pre-Approved Credentials							√	√	
Audit Trail establishment and control				√	√	√	√	√	√

8 Authentication Protocols

An authentication protocol is a defined sequence of messages between a claimant and a verifier that enables the verifier to verify that the claimant possesses or has control of a valid token to establish his/her identity. An exchange of messages between a claimant and a verifier that results in the authentication (or authentication failure) of the claimant is a protocol run.

8.1 Protocol Threats

Some threats are specific to authentication protocols and others are more general attacks on the components of the system.

8.1.1 Authentication Protocol Threat Model

Registration Authorities, CSPs, verifiers and relying parties are ordinarily trustworthy (in the sense of correctly implemented and not deliberately malicious). However, claimants or their systems may not be trustworthy (or else we could simply trust their identity assertions). Moreover, while RAs, CSPs and verifiers are normally trustworthy, they are not invulnerable, or could become corrupted. Therefore, protocols that expose long-term authentication secrets more than is absolutely required, even to trusted entities should be avoided.

Protocol threats include:

- Eavesdroppers observing authentication protocol runs for later analysis. In some cases the eavesdropper may intercept messages between a CSP and a verifier, or other parties rather than between the claimant and the verifier. Eavesdroppers generally attempt to obtain tokens to pose as claimants;
- Impostors:
  - impostor claimants posing as subscribers to verifiers;
  - impostor verifiers posing as verifiers to legitimate subscriber claimants to obtain tokens that can then be used to impersonate subscribers to legitimate verifiers;
  - impostor relying parties posing as the Federal IT system to verifiers to obtain sensitive user information;
- Hijackers who take over an already authenticated session to then:
  - pose as subscribers to relying parties to learn sensitive information or input invalid information;
  - pose as relying parties to verifiers to learn sensitive information or output invalid information.

Eavesdroppers are assumed to be physically able to intercept authentication protocol runs; however, the protocol may be designed to render the intercepted messages unintelligible, or to resist analysis that would allow the eavesdropper to obtain information useful to impersonating the claimant. Subscriber impostors need only normal communications access to verifiers or relying parties. Impostor verifiers may have special network capabilities to divert, insert or delete packets, but, in many cases, such attacks can be mounted simply by tricking subscribers with incorrect links in e-mails or on web pages, or by using domain names similar to those of relying parties or verifiers, and therefore the impostors need not necessarily have any unusual

network capabilities. Hijackers must be able to divert communications sessions, but this capability may be comparatively easy to achieve today when many subscribers use wireless network access.

Specific attack mechanisms on authentication protocols include:

- Eavesdroppers who listen passively to the authentication protocol exchange, and then attempt to learn secrets, such as passwords or keys.
- Active on-line attacks against authentication mechanisms including:
  - "In-band" attacks where the attacker assumes the role of a claimant with a genuine verifier. These include:
    - Password guessing attacks, where an impostor attempts to guess a password in repeated logon trials and succeeds when he/she is able to log onto a system. A targeted guessing attack is an attack against the password of a selected user whose name is known.
    - Replay attacks, where an attacker replays some part of a previous good protocol run to the verifier.
  - Out-of-band attacks where the attacker alters the authentication channel in some way such as:
    - Hijacking sessions after authentication is complete;
    - Verifier impersonation attacks where the attacker impersonates the verifier and induces the claimant to reveal his secret token;
    - Man-in-the middle attacks where the attacker inserts himself in the path of an authentication exchange, to obtain secret tokens.

8.1.2 Resistance to Protocol Threats

This section defines the meaning of resistance to specific protocol threats.

- *Eavesdropping resistance*: An authentication protocol is resistant to eavesdropping attacks if an eavesdropper who records all the messages passing between a claimant and a verifier or relying party finds that it is impractical to learn the private key, secret key or password or to otherwise obtain information that would allow the eavesdropper to impersonate the claimant. Eavesdropping resistant protocols make it impractical[3] for an attacker to carry out an off-line attack where he/she records an authentication protocol run then analyses it on his/her own system for an extended period, for example by systematically attempting to try every password in a large dictionary, or by brute force exhaustion.
- *Password guessing resistance*: An authentication protocol is resistant to password guessing attacks if it is impractical for the attacker with no *a priori* knowledge of the password to find the password by repeated authentication attempts with guessed passwords. Both the entropy of the password and the protocol itself contribute to this property. Password authentication systems can make password guessing impractical by

[3] "Impractical" is used here in the cryptographic sense of nearly impossible, that is there is always a small chance of success, but even the attacker with vast resources will nearly always fail. For off-line attacks, impractical means that the amount of work required to "break" the protocol is at least on the order of 2^{80} operations. For on-line attacks impractical means that the number of possible on-line trials is very small compared to the number of possible key or password values.

requiring use of high-entropy passwords (see Appendix A) and limiting the number of unsuccessful authentication attempts, or by throttling the rate at which attempts can be carried out.

- *Replay resistance*: An authentication protocol resists replay attacks if it is impractical to achieve a successful authentication by replaying a previous authentication message.
- *Hijacking resistance*: A property of both the authentication protocol and the subsequent session protocol used to transfer data. An authentication and transfer protocol in combination is resistant to hijacking if the authentication is bound to the transfer in a manner that prevents an adversary capable of inserting, deleting, or rerouting messages from altering the contents of any information sent between the claimant and the relying party without being detected. This is usually accomplished through the generation of a per-session shared secret in the claimant and the relying party and the subsequent use of the shared secret to authenticate the transfer of all sensitive information.
- *Verifier impersonation resistance*: In a verifier impersonation attack, the attacker poses as a legitimate verifier. It may be comparatively easy to impersonate a verifier by "name spoofing," or some more advanced network attack may be required (wireless LAN access today makes these "advanced" network attacks relatively easy for attackers in many circumstances). An authentication protocol is resistant to verifier impersonation if the impersonator does not learn the value of any secret or private token when acting as the verifier.
- *Man-in-the-middle resistance*: In a man-in-the-middle attack, the attacker poses as the verifier or relying party to the claimant, and as the claimant to the verifier or relying party and thereby learns or is able to alter sensitive information (especially passwords). Protocols are resistant to a man-in-the-middle attack when both parties (e.g., claimant and verifier) are authenticated to the other in a manner that prevents the participation of a third party.

8.1.3 Other Threats

Attacks are not limited to attacks against the authentication protocol itself. Other threats include:

- Insider threats that may compromise authentication tokens;
- Intrusion attacks that obtain credentials or tokens by penetrating the subscriber/claimant, CSP or verifier system;
- Out–of-band attacks that obtain tokens in some other manner, such as social engineering to get a subscriber to reveal his password, or "shoulder-surfing."

Insider threats are a major concern in many IT systems; however, good security, personnel, and auditing practices may mitigate these risks. General good practice to mitigate insider threats is outside the scope of this document.

From a protocol perspective, shared secrets must be closely held and carefully protected by CSPs. In general, at assurance Levels 2, 3 and 4 independent verifiers must not be given long-term shared secrets by CSPs, as this increases exposure to insider attacks. Independent verifiers may be given one time challenge-response information, provided that the shared secret is a

cryptographic key[4]. If the shared secret is a password, challenge-response mechanisms are vulnerable to insider or penetration attacks.

Network intrusion attacks are similar in many ways to insider threats, and are a risk for all on-line IT systems. Much information is available on the use of preventive measures such as firewalls, system configuration, and intrusion detection to mitigate the risks of network intrusion attacks (see sections 9.2 and 9.3 for some helpful references). Note that subscriber/claimant systems are also subject to network intrusion attacks, and strong authentication itself is one tool for blocking intrusion attacks.

This document is primarily concerned with the possibility that a network intrusion attack might allow an attacker to gain possession or control of tokens used in authentication protocols. The attack could either be against an individual client machine, or a verifier and the passwords or tokens of all the subscribers to that system. A general treatment of methods for mitigating intrusion attacks is outside the scope of this document. However, as with insider threats, some elements of the design of an authentication service can increase or mitigate penetration risks to the authentication service itself. Hardware tokens and cryptographic modules provide protection for keys and passwords against penetration attacks, because of the constrained environment that holds the keys. Most other authentication mechanisms are vulnerable to an attacker who has access to or can penetrate the claimant's system; however shared secret mechanisms are often vulnerable to penetration attacks against the verifier or CSP as well, where the attacker can find files of many shared secrets, while public key mechanisms are usually less vulnerable to attacks against verifiers or CSPs. Encryption of files of long-term shared secrets reduces the risks of a successful penetration attack.

8.2 Authentication Mechanism Levels

This section covers the mechanical authentication process of a subscriber /claimant who has registered his token with a CSP. Identity proofing and registration are dealt with separately in Section 7.

Four assurance levels are defined, numbered 1 to 4. Level 4 provides the highest level of authentication assurance, while Level 1 provides the least assurance. The characteristics of each level are summarized below, and described in detail in the following sections.

8.2.1 Level 1

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and permits the use of any token methods of Levels 2, 3 or 4, including PINS. Successful authentication requires that the claimant shall prove through a secure authentication protocol that he/she controls the token.

[4] Cell phone systems commonly employ such shared secret challenge-response authentication mechanisms. A shared secret key is maintained on the cell phone and at the home service provider's "home location register." When a user roams and registers with a base station of another host provider, the home service provider generates a challenge and a reply and sends it to the host service provider to be used to authenticate the roaming user. If the shared secret keys have sufficient entropy, insider offline attacks at the host service provider are impractical.

Plaintext passwords or secrets shall not be transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline analysis by eavesdroppers. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange will be able to find the password with a straightforward dictionary attack. Therefore there is not a requirement at this level to use FIPS approved cryptographic techniques.

At Level 1 long-term shared authentication secrets may be revealed to verifiers. Session tokens issued to claimants as a result of a successful authentication shall either be cryptographically authenticated by relying parties, (using FIP approved methods) or shall be obtained directly from the verifier via an authenticated protocol that meets Level 3 or Level 4.

8.2.1.1 Credential Lifetime, Status or Revocation

There are no stipulations about the revocation or lifetime of credentials at Level 1.

8.2.1.2 Protection of Long-term Shared Secrets

Files of shared secrets used by verifiers at Level 1 authentication shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords; typically they contain a one-way hash or "inversion" of the password.

8.2.1.3 Password Strength

For password (or PIN) based Level 1 authentication systems, the probability of success of a targeted on-line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed 2^{-11} (1 in 2048), over the life of the password. Appendix A contains information about estimating the entropy of passwords.

8.2.1.4 Example Implementations

A wide variety of technologies should be able to meet the requirements of Level 1. For example, a verifier might obtain a subscriber password from a CSP and authenticate the claimant by use of a challenge-response protocol.

8.2.2 Level 2

Level 2 allows a wide range of available authentication technologies to be employed and permits the use of any of the token methods of Levels 3 or 4, as well as passwords. Successful authentication requires that the claimant shall prove through a secure authentication protocol that he/she controls the token. Eavesdropper, replay, and on-line guessing attacks shall be prevented. FIPS approved cryptography is required.

8.2.2.1 Credential and Token Lifetime, Status or Revocation

CSPs shall provide a secure mechanism, such as a digitally signed revocation list or a status responder, to allow verifiers or relying parties to ensure that the credentials are still valid. Verifiers or relying parties shall check to ensure that the credentials they use are either freshly generated or still valid.

CSPs shall provide a mechanism to revoke subscribers within 72 hours after being notified that a credential is no longer valid to ensure that a claimant cannot successfully be authenticated. If the CSP issues credentials that expire automatically within 72 hours than the CSP shall not be

required to provide a mechanism to revoke them. For example, CSPs that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours and that the use of that password in authentication shall fail.

CAs cross-certified with the Federal Bridge CA at the Basic, Medium, High, Citizen and Commerce Class, or Common Certificate Policy levels are considered to meet credential status and revocation provisions of this level.

8.2.2.2 Assertion Lifetime and Status

Relying parties may accept assertions that are:

- digitally signed by the verifier; or
- obtained directly from the verifier via a Level 3 or Level 4 authentication protocol;
- obtained from a trusted repository via a Level 3 or Level 4 authentication protocol.

Assertions generated by a verifier shall expire after 12 hours and should not be used by the relying party.

8.2.2.3 Protection of Long-term Shared Secrets

Long term shared authentication secrets, if used, shall never be revealed to any party except the subscriber and CSP, however session (temporary) shared secrets may be provided to verifiers or relying parties by the CSP.

Files of shared secrets used by CSPs at Level 2 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords or secret; two alternative methods may be used to protect the shared secret:

1. Passwords may be concatenated to a salt and/or username and then hashed with a FIPS-approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashes are then stored in the password file.

2. Store shared secrets in encrypted form using approved encryption algorithms and modes and decrypt the needed secret only when immediately required for authentication. In addition any method allowed to protect shared secrets at Level 3 or 4 may be used at Level 2.

8.2.2.4 Password Strength

For password based Level 2 authentication systems, the probability of success of an on-line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed 2^{-16} (1 in 65,536), over the life of the password. Appendix A contains information about estimating the entropy of passwords.

8.2.2.5 Example Implementations

A wide variety of technologies can meet the requirements of Level 2. For example, a verifier might authenticate a claimant who provides a password through a secure (encrypted) TLS protocol session (tunneling). This prevents eavesdropper attacks, but not man-in-the middle

attacks. The verifier then puts a security assertion for the claimant in a secure server, and sends a "handle" for that assertion to a relying party in an HTTP referral.

8.2.3 Level 3

Level 3 authentication is based on proof of possession of a key or password through a cryptographic protocol. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or password) against compromise by the following protocol threats defined in section 8.1.1 above: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. In addition to Level 4 hard cryptographic tokens, the three kinds of tokens described below may be used to meet Level 3 requirements:

Soft cryptographic token: a cryptographic key stored on a general-purpose computer. Hardware tokens validated at FIPS 140-2 level 1 or higher may also be used to hold the key and perform cryptographic operations. The claimant shall be required to activate the key before using it with a password or biometric. Authentication requires that the claimant shall prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however, session (temporary) shared secrets may be provided to verifiers by the CSP. FIPS approved cryptographic techniques shall be used for all operations. All sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. As required, data may also optionally be encrypted under keys derived in the authentication process (note: encryption does not guarantee authentication). Relying parties must determine which data requires authentication or confidentiality protection, and are not required to authenticate or encrypt all data transferred.

One-time password device tokens: the authentication depends on a symmetric key stored on a personal hardware device that is a cryptographic module validated at FIPS 140-2 level 1 or higher. The device combines a nonce with a cryptographic key to produce an output that is sent to the verifier as a password. The password shall be used only once and is cryptographically generated; therefore it needs no additional eavesdropper protection. The one-time password shall have at least 10^6 possible values. To protect against the use of a stolen token, one of 3 measures shall be used:

- A user-entered password is required to activate the token;
- The token contains a biometric reader (e.g., fingerprint reader) that is used to activate the device;
- The claimant also sends the verifier a personal password with the one-time password; in this case the personal password shall meet the requirements for Level 2.

Password tokens: passwords used for Level 3 authentication shall be used in zero knowledge password protocols (i.e., neither verifiers nor claimants learn anything about the password not already known to them from an authentication attempt) that result in a shared cryptographic strength key and an eavesdropper is faced with an attack as difficult as an exhaustive attack on an 80-bit symmetric key to recover the key or determine the password.

Authentication requires that the claimant shall prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP, however session (temporary) shared secrets may be provided to verifiers by the CSP. FIPS approved cryptographic techniques shall be used for all operations. All sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. As required, data may also optionally be encrypted under keys derived in the authentication process (note: encryption does not guarantee authentication). Relying parties must determine which data requires authentication or confidentiality protection, and are not required to authenticate or encrypt all data transferred.

Each of the three token types has somewhat different utility and security properties. Soft token solutions are easily realized in "thin clients" with TLS and client certificates. Moreover this solution allows not only initial authentication of claimants, but also allows the entire session, or as much of it as is security critical, to be cryptographically authenticated. Soft token solutions are vulnerable to an intruder with access who makes an undetected copy of the token and attacks the password that protects the token offline. Zero knowledge password solutions are not widely implemented in current off- the-shelf software, and are vulnerable to keyboard recording or "shoulder surfing" attacks that can compromise passwords; however no copy of the token should exist on the user's system to be stolen. One-time password device token systems are commercially available, portable and work easily with any browser client. They have the disadvantage that they do not generate a key as a part of authentication that can authenticate the entire session, and therefore are more vulnerable to man-in-the-middle or session hijacking type attacks, although such attacks will not reveal the authentication key. They have the security advantage that the token is a tangible, physical object, subscribers should know if their token is stolen, and the key is not vulnerable to network, shoulder-surfing or keyboard sniffer attacks.

All three token types present the eavesdroppers with similar strong cryptographic protection. Each has its advantages and disadvantages against other types of attacks. All three offer considerably greater strength than Level 2 solutions. Application implementers with specific Level 3 authentication requirements, who need to select a particular technology should chose the one that best suits the functional needs and risks of their application.

8.2.3.1 Credential/Token Lifetime, Status or Revocation

CSPs shall provide a secure mechanism to allow verifiers or relying parties to ensure that the credentials are valid. Such mechanisms may include: revocation lists, on-line validation servers, and the use of credentials with short life-times or the involvement of CSP servers that have access to status records in authentication transactions. Verifiers shall check to ensure that the credentials they use are either freshly issued or still valid.

CSPs shall have a procedure to revoke long-term shared secret tokens within 24 hours. The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the Basic, Medium, High or Common Certificate Policy levels are considered to meet credential status and revocation provisions of this level.

Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid.

At this level, sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.

8.2.3.2 Protection of Long-term Shared Secrets

Files of long-term shared secrets used by CSPs or verifiers at Level 3 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall be encrypted so that:

1. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.

2. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module.

3. Shared secrets are split by a cryptographic secret sharing method between *m* separate verifier systems, so that the cooperation of *n* (where $2 \leq n \leq m$) systems in a secure protocol is required to perform the authentication and an attacker who learns *n*-1 of the secret shares, learns nothing about the secret (except, perhaps, its size).

Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party verifiers, in an appropriate protocol, but long-term shared secrets shall not be shared with any third parties, including third party verifiers. Session authentication keys are typically created by cryptographically combining the long term shared secret with a nonce challenge, to generate a session key. The challenge and session key are securely transmitted to the verifier. The verifier in turn sends only the challenge to the claimant, and the claimant applies the challenge to the long-term shared secret to generate the session key. Both claimant and verifier now share a session key, which can be used for authentication. Such protocols are permitted at this level provided that all keys preserve at least 80-bits of entropy and approved cryptographic primitives (e.g., AES, SHA-1, SHA256, HMAC) are used for all operations.

8.2.3.3 Password Strength

For zero-knowledge password based Level 3 authentication systems, the probability of success of a targeted on-line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed 2^{-20} (1 in 1,048,576), over the life of the password. Appendix A states the method for estimating the entropy of passwords.

One-time passwords shall have at lest 10^6 possible values. If personal passwords are used by verifiers in conjunction with one-time passwords, the personal passwords shall meet the requirements for passwords used with Level 2. The strength of passwords used to activate one-time password devices is not specified.

8.2.3.4 Example Implementations

Level 3 assurance can be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key certificates. Other protocols with similar properties can also be used.

8.2.4 Level 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that "hard" cryptographic tokens are required. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or above. By requiring a physical token, which cannot readily be copied and which shall be unlocked with a password or biometric, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant shall prove through a secure authentication protocol that he controls the token. The protocol threats defined in section 8.1.1 above (eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks) shall be prevented. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or relying parties by the CSP. Strong, FIPS approved cryptographic techniques shall be used for all operations. All sensitive data transfers shall be cryptographically authenticated using keys derived in the authentication process.

8.2.4.1 Credential/Token Lifetime, Status or Revocation

CSPs shall provide a secure mechanism to allow verifiers or relying parties to ensure that the credentials are valid. Such mechanisms may include: revocation lists, on-line validation servers, and the use of credentials with short life-times or the involvement of CSP servers that have access to status records in authentication transactions. Verifiers shall check to ensure that the credentials they use are either freshly issued or still valid.

CSPs shall have a procedure to revoke credentials within 24 hours. Verifiers or relying parties shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid. The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the High and Common Certificate Policies shall be considered to meet credential status provisions of Level 4. [FBCA1].

At this level sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.

8.2.4.2 Protection of Long-term Shared Secrets

Files of long-term shared secrets used by CSPs or verifiers at Level 4 shall be protected in the same manner as long-term shared secrets for Level 3 (specified in section 8.2.3.2 above)

8.2.4.3 Password Strength

Password based primary authentication is not allowed at Level 4. Hardware tokens at Level 4 shall be FIPS 140-2 Level 2 or higher tokens and shall meet the PIN/password requirements of FIPS 140-2 to unlock the tokens.

8.2.4.4 Example Implementations

Level 4 assurance can be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key hard tokens. Other protocols with similar properties can also be used.

8.2.5 Summary of Mechanism Requirements by level

Table 1. Allowed Token Types

	Level 1	**Level 2**	**Level 3**	**Level 4**
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time password device	√	√	√	
Strong password	√	√		
PIN	√			

Table 2. Required Protections

	Level 1	**Level 2**	**Level 3**		**Level 4**
			Soft or ZKP	1TPD	
Protection against					
Eavesdropper		√	√	√	√
Replay	√	√	√	√	√
On-line guessing	√	√	√	√	√
Verifier impersonation			√	*	√
Man-in-the-middle			√	*	√
Session hijacking			√		√

* partial protection; MIM or impostor verifier may learn password, but not primary secret authentication key

Table 3. Authentication Protocol Types

	Level 1	Level 2	Level 3	Level 4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Zero knowledge password	√	√	√	
Tunneled password	√	√		
Challenge-response password	√			

Table 4. Required Properties

	Level 1	Level 2	Level 3	Level 4
Shared secrets not reveled to 3rd parties		√	√	√
Sensitive data transfer authenticated			√	√

9 References

9.1 General References

[OMB 04-04] OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 16, 2003, available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[OMB 03-22] OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003 available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[RFC 2246] IETF, RFC 2246, *The TLS Protocol, Version 1.0*. January 1999, available at: http://www.ietf.org/html.charters/tls-charter.html

[RFC2560] IETF, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, available at: http://www.ietf.org/html.charters/pkix-charter.html

[RFC 3280] IETF, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, available at: http://www.ietf.org/html.charters/pkix-charter.html

[RFC 3546] IETF, RFC 3546, Transport Layer Security (TLS) Extensions, June 2003, available at: http://www.ietf.org/html.charters/tls-charter.html

9.2 NIST ITL Bulletins

NIST ITL Bulletins are available at: http://csrc.nist.gov/publications/nistbul/index.html. The following bulletins may be of particular interest to those implementing systems of applications requiring e-authentication.

[ITL Dec02] ITL Bulletin, *Security of Public Webservers*, Dec. 2002

[ITL July02] ITL Bulletin, *Overview: The Government Smartcard Interoperability Specification*, July 02

[ITL Jan02] ITL Bulletin, *Guideline on Firewalls and Firewall Policy*, January 2002

[ITL Feb00] ITL Bulletin, *Guideline for Implementing Cryptography in the Federal Government*, February 2000

[ITL Dec99] ITL Bulletin, *Operating System Security: Adding to the Arsenal of Security Techniques*, December 1999

[ITL Nov99] ITL Bulleting, *Acquiring and Deploying Intrusion Detection Systems*, November 1999

[ITL Sep99] ITL Bulletin, *Securing Web Servers*, September 1999

[ITL May99] ITL Bulletin, *Computer Attacks: What They Are and How to Defend Against Them*, May 1999

9.3 NIST Special Publications

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html. The following publications may be of particular interest to those implementing systems of applications requiring e-authentication.

[SP 800-31] NIST Special Publication, 800-31, *Intrusion Detection Systems (IDS)*, November 2001

[SP 8000-33] NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001

[SP 800-40] NIST Special Publication 800-40, *Procedures for Handling Security Patches*, September 2002

[SP 800-41] NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002

[SP 800- 42] NIST Special Publication 800-42, *Guideline on Network Security Testing*, draft

[SP 800-43] NIST Special Publication 800-43, *Guide to Securing Windows 2000 Professional*, November 2002

[SP 800-44] NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002

[SP 800- 47] NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002

[SP 800- 52] NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security Implementations, draft.

9.4 Federal Information Processing Standards

FIPS can be found at: http://csrc.nist.gov/publications/fips/

[FIPS 46-3] Federal Information Processing Standard Publication 46-3, *Data Encryption Standard (DES)*, NIST, October 25, 1999

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001

[FIPS 180-2] Federal Information Processing Standard Publication 180-2, *Secure Hash Standard (SHS)*, NIST, August 2002.

[FIPS186-2] Federal Information Processing Standard Publication 186-2, *Digital Signature Standard (DSS)*, NIST, June 2000.

[FIPS 197] Federal Information Processing Standard Publication197, *Advanced Encryption Standard (AES)*, NIST, November 2001.

[FIPS 198] Federal Information Processing Standard Publication 198, *Keyed-Hash Message Authentication Code (HMAC)*, NIST, March 2002.

9.5 Certificate Policies

These certificate policies can be found at: http://www.cio.gov/fbca/library.htm.

[FBCA1] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*

[FBCA2] *Citizen & Commerce Certificate Policy*

[FBCA3] *X.509 Certificate Policy for the Common Policy Framework*

Appendix A: Estimating Password Entropy and Strength

Claude Shannon coined the use of the term "entropy[i]" information theory. The concept has many applications to information theory and communications and Shannon also applied it to express the amount of actual information in English text. Shannon says, "The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary digits (0 or 1) in the most efficient way, the entropy H is the average number of binary digits required per letter of the original language."[ii]

Entropy in this sense is at most only loosely related to the use of the term in thermodynamics. A mathematical definition of entropy in terms of the probability distribution function is:

$$H(X) := -\sum_{x} P(X = x) \log_2 P(X = x)$$

where *P(X=x)* is the probability that the variable *X* has the value *x*.

Shannon was interested in strings of ordinary English text and how many bits it would take to code them in the most efficient way possible. Since Shannon coined the term, "entropy" has been used in cryptography as a measure of the difficulty in guessing or determining a password or a key. Clearly the strongest key or password of a particular size is a truly random selection, and clearly, on average such a selection cannot be compressed. However it is far from clear that compression is the best measure for the strength of keys and passwords, and cryptographers have derived a number of alternative forms or definitions of entropy, including "guessing entropy" and "min-entropy." As applied to a distribution of passwords the guessing entropy is, roughly speaking, an estimate of the average amount of work required to guess the password of a selected user, and the min-entropy is a measure of the difficulty of guessing the easiest single password to guess in the population.

If we had a good knowledge of the frequency distribution of passwords chosen under a particular set of rules, then it would be straightforward to determine either the guessing entropy or the min-entropy of any password. An attacker who knew the password distribution would find the password of a chosen user by first trying the most probable password for that chosen username, then the second most probable password for that username and so on in decreasing order of probability until he found the password that worked with the chosen username. The average for all passwords would be the guessing entropy. The attacker who is content to find the password of any user would follow a somewhat different strategy, he would try the most probable password with every username, then the second most probable password with every username, until he found the first "hit." This corresponds to the min-entropy.

Unfortunately, we do not have much data on the passwords users choose under particular rules, and much of what we do know is found empirically by "cracking" passwords, that is by system administrators applying massive dictionary attacks to the files of hashed passwords (in most systems no plaintext copy of the password is kept) on their systems. NIST would like to obtain more data on the passwords users actually choose, but, where they have the data, system administrators are understandably reluctant to reveal password data to others. Empirical and

anecdotal data suggest that many users choose very easily guessed passwords, where the system will allow them to do so.

A.1 Randomly Selected Passwords

As we use the term here, "entropy" denotes the uncertainty in the value of a password. Entropy of passwords is conventionally expressed in bits. If a password of *k* bits is chosen at random there are 2^k possible values and the password is said to have *k* bits of entropy. If a password of length *l* characters is chosen at random from an alphabet of *b* characters (for example the 94 printable ISO characters on a typical keyboard) then the entropy of the password is b^l (for example if a password composed of 8 characters from the alphabet of 94 printable ISO characters the entropy is $94^8 \approx 6.9 \times 10^{15}$ – this is about 2^{52}, so such a password is said to have about 52 bits of entropy). For randomly chosen passwords, guessing entropy, min-entropy, and Shannon entropy are all the same value. The general formula for entropy, *H* is given by:

$$H = \log_2 (b^l)$$

Table A.1 gives the entropy versus length for a randomly generated password chosen from the standard 94 keyboard characters (not including the space). Calculation of randomly selected passwords from other alphabets is straightforward.

A.2 User Selected Passwords

A.2.1 Shannon Entropy as an Estimate of Guessing Entropy

It is much more difficult to estimate the entropy in passwords that users choose for themselves, because they are not chosen at random and they will not have a uniform random distribution. Passwords chosen by users probably roughly reflect the patterns and character frequency distributions of ordinary English text, and are chosen by users so that they can remember them. Experience teaches us that many users, left to choose their own passwords will choose passwords that are easily guessed, and even fairly short dictionaries of a few thousand commonly chosen passwords, when they are compared to actual user chosen passwords, succeed in "cracking" a large share of those passwords.

In this guidance, we have chosen to use Shannon's estimate of the entropy in ordinary English text as the starting point to estimate the entropy of user-selected passwords. It is a big assumption that passwords are quite similar to other English text, and it would be better if we had a large body of actual user selected passwords, selected under different composition rules, to work from, but we have no such resource, and it is at least plausible to use Shannon's work for a "ballpark" estimate. Readers are cautioned against interpreting the following rules as anything more than a very rough rule of thumb method to be used for the purposes of e-Authentication.

We are treating Shannon entropy estimates as guessing entropy, which it seems closes to, and it is arguable that it would be better to use a min-entropy based estimate, which would be considerably lower and bear a closer relationship to the risk that systems might be penetrated, while guessing entropy is more closely related to targeted attacks on individuals. In the body of

this guidance we have select conservative (high entropy) thresholds to compensate for the greater risk to systems, compensate for the higher values of guessing entropy (as opposed to min-entropy). Moreover, it is the risk to users that they might be attacked and impersonated that is most important to e-Authentication users.

A.2.2 Basic Dictionary Test

However, ordinary English text is not chosen to be easily remembered, and experience suggests that a significant share of users will chose passwords that are very easily guessed ("password" may be the most commonly selected password, where it is allowed). Suppose, for example, that 1 user in 1000 chooses one of the 2 most common passwords, in a system that allows a user 3 tries before locking a password. An attacker with a list of user names can use an automated attack to try those 2 passwords with each user name, and can expect to succeed half the time in about user 700 trials. Clearly this is a practical attack if the only goal is to get access to the system, rather than to impersonate a single selected user. This is usually too dangerous a possibility to ignore; therefore the baseline constraints applied against all passwords of 12 characters or less are that a basic dictionary test is applied as follows:

- Upper case letters in passwords are converted to entirely lower case and compared to a basic dictionary of at least 1000 commonly selected otherwise legal passwords and rejected if they match any dictionary entry, and
- Passwords that are detectable permutation of the username are not allowed.

This basic dictionary test probably has relatively little effect on the guessing or Shannon entropy of the passwords, but may significantly increase the min-entropy and the effort required to break into a system.

A.2.3 Entropy Estimates

Shannon conducted experiments where he gave people strings of English text and asked them to guess the next character in the string. From this he estimated the entropy of each successive character. He used a 27-character alphabet, the ordinary English lower case letters plus the space.

In the following discussion we assume that passwords are user selected from the normal keyboard alphabet of 94 printable characters, and are at least 6-characters long. Since Shannon used a 27 character alphabet it may seem that the entropy of user selected passwords would be much larger, however the assumption here is that users will choose passwords that are almost entirely lower case letters, unless forced to do otherwise, and that rules that force them to include capital letters or non-alphabetic characters will generally be satisfied in the simplest and most predictable manner, often by putting a capital letter at the start (as we do in ordinary English) and punctuation or special characters at the end, or by some simple substitution, such as $ for the letter "s." Moreover rules that force passwords to appear to be highly random will be counterproductive because they will make the passwords hard to remember. Users will then write the passwords down and keep them in a convenient (that is insecure) place, such as pasted on their monitor. Therefore it is reasonable to start from estimates of the entropy of simple English text, assuming only a 27-symbol alphabet.

Shannon observed that, although there is a non-uniform probability distribution of letters, it is comparatively hard to predict the first letter of an English text string, but, given the first letter, it is much easier to guess the second and given the first two the third is easier still, and so on. He estimated the entropy of the first symbol at 4.6 to 4.7 bits, declining to on the order of about 1.5 bits after 8 characters. Very long English strings (for example the collected works of Shakespeare) have been estimated to have as little as .4 bits of entropy per character.[iii] Similarly, in a string of words, it is harder to predict the first letter of a word than the following letters, and the first letter carries about 6 times more information than the 5th or later letters[iv]

An attacker attempting to find a password will try the most likely chosen passwords first. Very extensive dictionaries of passwords have been created for this purpose. Because users often choose common words or very simple passwords systems commonly impose rules on password selection in an attempt to prevent the choice of "bad" passwords and improve the resistance of user chosen passwords to such dictionary or rule driven password guessing attacks. For the purposes of this guidance we break those rules into two categories:

1. dictionary tests that test prospective passwords against an "extensive dictionary test" of common words and commonly used passwords, then disallow passwords found in the dictionary. We do not precisely define an extensive dictionary test, since it must be tailored to the password length and rules, but it should prevent selection of passwords that are simple transformations of any one word found in an unabridged English dictionary. There is no intention to prevent selection of long passwords (16 characters or more based on phrases) and no need to impose a dictionary test on such long passwords.
2. composition rules that typically require users to select passwords that include lower case letters, upper case letters, and non-alphabetic symbols (e.g.;: "~!@#$%^&*()_-+={}[]|\:;'<,>.?/1234567890").

Either dictionary tests or composition rules eliminate some passwords and reduce the space that an adversary must test to find a password in a guessing or exhaustion attack. However they can eliminate many obvious choices and therefore we believe that they generally improve the "practical entropy" of passwords, although they reduce the work required for a truly exhaustive attack.

Table A.1 provides a rough estimate of the average entropy of user chosen passwords as a function of password length. Estimates are given for user selected passwords drawn from the normal keyboard alphabet that are not subject to further rules, passwords subject to a composition rule that requires non-alphabetic characters, passwords subject to a dictionary check to prevent the use of common words or commonly chosen passwords and passwords subject to both composition rules and a dictionary test. In addition an estimate is provided for passwords or PINs with a ten-digit alphabet. The table also shows the calculated entropy of randomly selected passwords and PINs. The values of Table A.1 should not be taken as accurate estimates of absolute entropy, but they do provide a rough relative estimate of the likely entropy of user chosen passwords, and some basis for setting a standard for password strength.

The logic of the Table A.1 is as follows for user-selected passwords drawn from the full keyboard alphabet:

- the entropy of the first character is taken to be 4 bits;
- the entropy of the next 7 characters are 2 bits per character; this is roughly consistent with Shannon's estimate that "when statistical effects extending over not more than 8 letters are considered the entropy is roughly 2.3 bits per character;"
- for the 9th through the 20th character the entropy is taken to be 1.5 bits per character;
- for characters 21 and above the entropy is taken to be 1 bit per character;
- A "bonus" of 6 bits of entropy is assigned for a composition rule that requires upper case and non-alphabetic characters. This forces the use of these characters, but in many cases thee characters will occur only at the beginning or the end of the password, and it reduces the total search space somewhat, so the benefit is probably modest and nearly independent of the length of the password;
- A bonus of up to 6 bits of entropy is added for an extensive dictionary check. If the attacker knows the dictionary, he can avoid testing those passwords, and will in any event, be able to guess much of the dictionary, which will, however, be the most likely selected passwords in the absence of a dictionary rule. The assumption is that most of the benefits for a dictionary test accrue to relatively short passwords, because any long password that can be remembered must necessarily be a "pass-phrase" composed of dictionary words, so the bonus declines to zero at 20 characters.

For user selected PINs the assumption of Table A.1 is that such pins are subjected at least to a rule that prevents selection of all the same digit, or runs of digits (e.g., "1234" or "76543"). This column of Table A.1 is at best a very crude estimate, and experience with password crackers suggests, for example, that users will often preferentially select simple number patterns and recent dates, for example their year of birth.

A.2 Other Types of Passwords

Some password systems require a user to memorize a number of images, such as faces. Users are then typically presented with successive fields of several images (typically 9 at a time), each of which contains one of the memorized images. Each selection represents approximately 3.17 bits of entropy. If such a system used five rounds of memorized images, then the entropy of system would be approximately 16 bits. Such systems are sometimes combined with a conventional PIN or password.

A.3 Examples

The intent of this guidance is to allow designers and implementers as much flexibility as possible in designing password authentication systems. System designers can trade off password length, rules and measures imposed to limit the number of guesses an adversary can attempt.

The approach of this recommendation to password strength is that it is a measure of the probability that an attacker, who knows nothing but a user's name, can discover the user's password by means of "in-band" password guessing attack. That is the attacker attempts to try different passwords until he/she authenticates successfully. At each level given below, the

maximum probability that, over the life of the password, an attacker with no *a priori* knowledge of the password will succeed in an in-band password guessing attack is:

1. Level 1- 2^{-11} (1 in 2048)
2. Level 2 - 2^{-16} (1 in 65,536)
3. Level 3 - 2^{-20} (1 in 1,048,576)

Consider a system that assigns subscribers 6 character passwords, randomly selected from an alphabet of 94 printable keyboard characters. From Table A.1 we see that such a password is considered to have 39.5 bits of entropy. If the authentication system limits the number of possible unsuccessful authentication trials to $2^{39.5}/2^{16} = 2^{23..5}$ trials, the password strength requirements of level 2 are satisfied. The authentication system could, for example, simply maintain a counter that locked the password after $2^{23.5}$ about ten million total unsuccessful trials. An alternative scheme would be to lock out the claimant for a minute after three successive failed authentication attempts. Such a lock out would suffice to throttle automated attacks to 3 trials a minute and it would take about 45 years to carryout $2^{23.5}$ trials. If the system required that passwords authentication attempts be locked for one minute after three unsuccessful trials and that passwords be changed every five years, then the requirements of level 2 would be comfortably satisfied.

Consider a system that used:

- a minimum of 8 character passwords, selected by subscribers from an alphabet of 94 printable characters,
- required subscribers to include at least one upper case letter, one lower case letter, one number and one special character, and;
- prevented subscribers from including common words or permutations of their username.

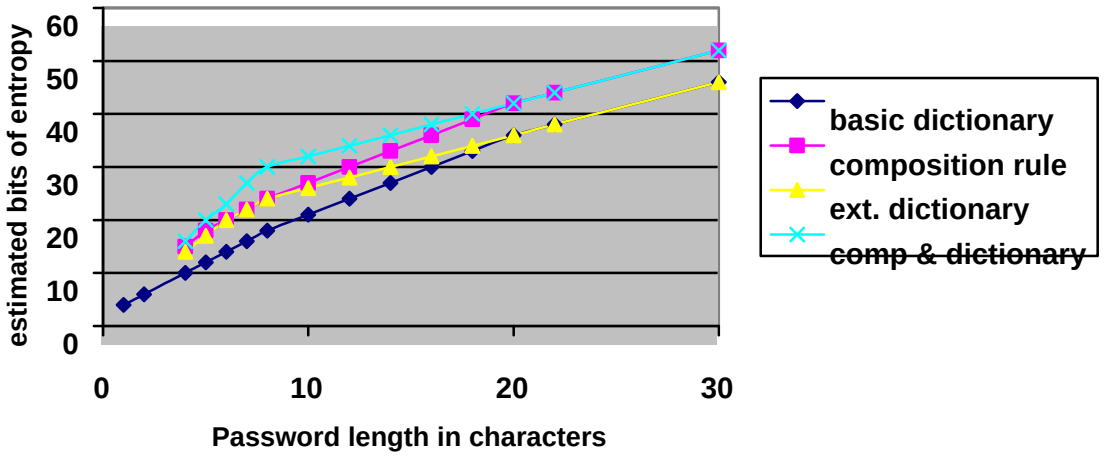
Such a password would meet the composition and dictionary rules for user-selected passwords in Appendix A, and from Table A.1 get estimated entropy of 30 bits. Any system that limited a subscriber to less than 2^{14} (16,384) failed authentication attempts over the life of the password would satisfy the requirements of level 2. For example, consider a system that required passwords to be changed every two years and limited trials by locking an account for 24 hours after 6 successive failed authentication attempts. An attacker could get $2 \times 365 \times 6 =$ 4,380 attempts during the life of the password and would meet the requirements of level 2.

It will be very hard to impose dictionary rules on longer passwords, and many people may prefer to memorize a relatively long “pass-phrases.” of words, rather than a shorter, more arbitrary password. An example might be: “IamtheCapitanofthePina4”.

As an alternative to imposing some arbitrary specific set of rules, an authentication system might grade user passwords, using the rules stated above, and accept any that meet some minimum entropy standard. For example, suppose passwords with at least 24-bits of entropy were required. We can calculate the entropy estimate of “IamtheCapitanofthePina4” by observing that the string has 23 characters and would satisfy a composition rule requiring upper case and non-alphabetic characters. Table A.1 estimates 45 bits of entropy for this password. This password would meet the rule.

Table A.1 – Estimated Password Entropy in bits vs. Password Length

	User Chosen					Randomly Chosen	
	94 character alphabet				10 char. alphabet		94 char alphabet
Length Char.	**Basic Dictionary Only**	**Comp. Rule & Basic Dict.**	**Extensive Dictionary**	**Extensive Dictionary and Comp. rule**			
1	4	-	-	-	3	3.3	6.6
2	6	-	-	-	5	6.7	13.2
3	8	-	-	-	7	10.0	19.8
4	10	15	14	16	9	13.3	26.3
5	12	18	17	20	10	16.7	32.9
6	14	20	20	23	11	20.0	39.5
7	16	22	22	27	12	23.3	46.1
8	18	24	24	30	13	26.6	52.7
10	21	27	26	32	15	33.3	65.9
12	24	30	28	34	17	40.0	79.0
14	27	33	30	36	19	46.6	92.2
16	30	36	32	38	21	53.3	105.4
18	33	39	34	40	23	59.9	118.5
20	36	42	36	42	25	66.6	131.7
22	38	44	38	44	27	73.3	144.7
24	40	46	40	46	29	79.9	158.0
30	46	52	46	52	35	99.9	197.2
40	56	62	56	62	45	133.2	263.4



[i] C. E. Shannon, "A mathematical Theory of Communication," *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October 1948, see http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

[ii] C. E. Shannon, "Prediction and Entropy of Printed English", *Bell System Technical Journal*, v.30, n. 1, 1951, pp. 50-64.

[iii] Thomas Schurmann and Peter Grassberger, "Entropy estimation of symbol sequences," http://arxiv.org/ftp/cond-mat/papers/0203/0203436.pdf

[iv] *ibid.*