NIST Special Publication 800-63
Version 1.0.2

Electronic Authentication Guideline

Recommendations of the National Institute of Standards and Technology

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

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

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2006

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

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

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 also 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.

National Institute of Standards and Technology Special Publication 800-63, 64 pages (April 2006)

Certain commercial entities, equipment, or material may be identified in the document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

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.

Acknowledgments

The authors, Bill Burr, Tim Polk and Donna Dodson of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Executive Summary

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. This recommendation provides technical guidance to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information. NIST expects to explore other means of remote authentication (for example using biometrics, or by extensive knowledge of private, but not truly secret, personal information) and may develop additional guidance on the use of these methods for remote authentication.

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:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of 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.

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. 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.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 2 – Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. 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 and PINs. 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.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Level 3- Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish

two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

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 only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, 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 verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to 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

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network. This recommendation provides technical guidance to agencies 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 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 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 criteria for determining the level of e-authentication assurance required for specific electronic transactions and systems, based on the risks and their likelihood of occurrence.

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

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of 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.

The overall authentication assurance level is determined by the lowest assurance level achieved in any of the four areas listed above.

This technical guidance covers remote electronic authentication of human users to Federal agency IT systems over a 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 in which their identity is bound to an authentication secret, called a token. Thereafter, the individuals are remotely authenticated to systems and applications over an open network, using the token in an authentication protocol. The authentication protocol allows an individual to demonstrate to a verifier that he has or knows the secret token, in a manner that protects the secret from compromise by different kinds of attacks. Higher authentication assurance levels require use of stronger tokens (harder to guess secrets) and better protection of the token from attacks. This 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). As this information is private but not actually secret, confidence in the identity of an individual can be hard to achieve. In addition, the complexity and interdependencies of knowledge based authentication systems are difficult to quantify. However, knowledge based authentication techniques are included as part of registration in this document.

Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example for entry into buildings. Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols

addressed in this document. In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret. The use of biometrics to "unlock" conventional authentication tokens and to prevent repudiation of registration is identified in this document.

NIST is continuing to study both the topics of knowledge based authentication and biometrics and may issue additional guidance on their uses for remote authentication of individuals across a network.

This document identifies minimum technical requirements for remotely authenticating identity. Agencies may determine based on their risk analysis that additional measures are appropriate in certain contexts. In particular, privacy requirements and legal risks may lead agencies to determine that additional authentication measures or other process safeguards are appropriate. When developing e-authentication processes and systems, agencies should consult *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* [OMB 03-22]. See the *Guide to Federal Agencies on Implementing Electronic Processes* for additional information on legal risks, especially those that related to the need to satisfy legal standards of proof and prevent repudiation [DOJ 2000].

4. Definitions and Abbreviations

Active Attack	An attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
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. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2. For more information on validation and alist of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/.
Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence in user identities.
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.
Biometric	An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Certificate Revocation	A list of revoked public key certificates created and digitally signed by

List (CRL)	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 claimant 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, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Credentials Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cryptographic key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number. See also Asymmetric keys, Symmetric key.
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 digitally 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.
Guessing entropy	A measure of the difficulty that an attacker has to guess the average password used in a system. In this document, entropy is stated in bits. When a password has n-bits of guessing entropy then an attacker has as much difficulty guessing the average password as in guessing an n-bit random quantity. The attacker is assumed to know the actual password frequency distribution. See Appendix A.
Hash function	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1. (One-way) It is computationally infeasible to find any input that maps to any pre-specified output, and 2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
HMAC	Hash-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-KDC exchange.
Man-in-the-middle attack (MitM)	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 uses a symmetric key to detect both accidental and intentional modifications of the data.
Min-entropy	A measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system. In this document, entropy is stated in bits. When a password has n-bits of min-entropy then an attacker requires as many trials to find a user with that password as is needed to guess an n-bit random quantity. The attacker is assumed to know the most commonly used password(s). See Appendix A.
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 either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be 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 secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
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 digitally 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 token (e.g., a key or password)
Protocol run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Public key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
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. The certificate indicates that the subscriber identified in the

	certificate has sole control and access to the private key. See also [RFC 3280]
Pseudonym	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.
Registration	The process through which a party applies to become a subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.
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 a 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.
Subject	The person whose identity is bound in a particular credential.
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 widely implemented in 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's public key certificate to (1) authenticate the verifier to the claimant, (2) establish an encrypted session between the verifier and claimant, and (3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers.
Verified Name	A subscriber name that has been verified by identity proofing.
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.

5. E-Authentication Model

In accordance with [OMB 04-04] e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet, however in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with *registration*. An *applicant* applies to a *Registration Authority (RA)* to become a *subscriber* of a *Credential Service Provider (CSP)* and, as a subscriber, is issued or registers a secret, called a *token*, and a *credential* that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

The subscriber's name may either be a *verified name* or a *pseudonym*. A verified name is associated with the identity of a real person and before an applicant can receive credentials or register a token associated with a verified name, 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 is performed by an RA that registers subscribers with the CSP. At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists *relying parties*, that is parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4.

In this guidance, the party to be authenticated is called a *claimant* and the party verifying that identity is called a *verifier*. 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 verify that the clamant is the subscriber. The verifier passes on an assertion about the identity of the subscriber to the relying party. That assertion includes identity information about a subscriber, such as the subscriber name, an identifier assigned at registration, or other subscriber attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application). Where the verifier is also the relying party, the assertion may be implicit. In addition, the subscriber's identifying information may be incorporated in credentials (e.g., public key certificates) made available by the claimant. The relying party can use the authenticated information provided by the verifier/CSP to make access control or authorization decisions.

Authentication simply establishes identity, or in some cases verified personal attributes (for example the subscriber is a US Citizen, is a student at a particular university, or is assigned a particular number or code by an agency or organization), 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, will use a subscriber's 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.

In summary, an individual applicant applies first to an RA. The RA identity proofs that applicant. As the result of successful identity proofing, the applicant becomes a subscriber of a CSP associated with the RA, with a credential and a secret token registered to the subscriber. When the subscriber needs to authenticate to perform a transaction, he or she becomes a claimant to a verifier. The claimant proves to the verifier that he or she controls the token, using an authentication protocol. If the verifier is separate from the relying party (application), the verifier provides an assertion about the claimant to the relying party, which uses the information in the assertion to make an access control or authorization decision. If the transaction is significant, the relying party may log the subscriber identity and credential(s) used in the authentication along with relevant transaction data.

5.1. Subscribers, RAs and CSPs

In the conceptual e-authentication model, a claimant in an authentication protocol is a subscriber to some CSP. At some point, an applicant registers with an RA, which verifies the identity of the applicant, 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 applicant (and possibly other verified attributes) to a CSP. The applicant then becomes a subscriber of the CSP.

The CSP establishes a mechanism to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber. 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 verified 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. Subscribers have a duty to maintain control of their tokens and comply with the responsibilities to the CSP. The CSP maintains registration records for each subscriber to allow recovery of registration records.

There is always a relationship between the RA and CSP. In the simplest and perhaps the most common 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 generically are something 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 is a secret and the token must be protected. The token may, for example, be a cryptographic key, that is protected by encrypting it under a password. An impostor must steal the encrypted key and learn the password to use the token.

Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

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

Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key. Such a device is considered to effectively provide two factor authentication, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key.

The secrets are often based on either *public key pairs* (asymmetric keys) or *shared secrets*. A *public key* and a related private key comprise a public key pair. The *private key* is used by the claimant as a token. A verifier, knowing the 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). 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 and 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. In this document, biometrics are used in the registration process to be able to later prevent a subscriber who in fact registered from repudiating the registration, to help identify those who commit registration fraud, and to unlock tokens. Biometrics are not used directly as tokens in this document.

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 credentials 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 a name 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. At a minimum, credentials include identifying information that permits recovery of the records of the registration associated with the credentials and a name that is associated with the subscriber. In every case, given the issuer and the identifying information in the credential, it must be possible to recover the registration records upon which the credentials are based. 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 that 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 data in a directory or database. These credentials may be digitally signed objects (e.g., X.509 certificates), in which case their integrity may be verified. In this case, the directory or database may be an untrusted entity, since the data it supplies is self-authenticating. Alternatively, the directory or database server may be a trusted entity that authenticates itself to the relying party or verifier. When the directory or database server is trusted, unsigned credentials may simply be stored as unsigned data.

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, with no knowledge of the token before the authentication protocol run, learns nothing about the token from the run. 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. It is undesirable for verifiers to learn shared secrets unless they are a part of the same entity as the CSP that registered the tokens. 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 contain, at a minimum, the name of the claimant, as well as identifying information that permits recovery of registration records. 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. SAML assertions may optionally be digitally signed.
- Cookies, character strings placed in a web browser's memory, are available to websites within the same Internet domain as the server that placed them in the web browser. Cookies are used for many purposes and may be assertions or may contain pointers to assertions.[1]

Assertions may be stored as directory or database objects. Where assertions are digitally signed objects (e.g., signed SAML assertions), their integrity may be verified.

[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.

Alternatively, the directory or database server may be a trusted, authenticated entity. When the server is trusted, unsigned assertions may be accepted based on the source.

5.6. Relying Parties

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 normally receives an assertion from the verifier. The relying party ensures that the assertion came from a verifier trusted by the relying party. The relying party also processes any additional information in the assertion, such as personal attributes or expiration times.

6. Tokens

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

- *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 key shall be encrypted under a key derived from some activation data. Typically, this activation data will be a password known only to the user, so a password is required to activate the token. For soft tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher, and may be either a hardware device or a software module. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

  Some "mobility solutions" also allow keys to be stored on servers and downloaded to subscriber systems as needed. Other mobility solutions employ key components generated from passwords with key components stored on servers for use in split signing schemes. Such solutions may provide satisfactory soft tokens, provided that a subscriber password or other activation data is required to download and activate the key, that the protocol for downloading the keys block eavesdroppers and man-in-the-middle attacks, and the authentication process produces Approved digital signatures or message authentication codes. These mobility solutions usually present what appear to relying parties to be ordinary PKI digital signatures, and may be acceptable under this recommendation provided they meet the PKI cross certification requirements. This cross certification will require a detailed analysis of the implementation of the specific mobility scheme.

- *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 an 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, a counter generated on the device, or a challenge from the verifier (if the device has an entry capability). The one-time password typically is displayed on the device and manually input to the verifier as a password (direct electronic input from the device to a computer is also allowed). The one-time password must have a limited lifetime, on the order of minutes, although the shorter the better.

- *Password token* – a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however some systems use a number of images that the subscriber memorizes and must identify when presented along with other similar images.

6.1. Token Threats

If an attacker can gain control of a token, they will be able to masquerade as the token's owner. Threats to tokens can be categorized into attacks on the three factors:

- *Something you have* may be stolen from the owner or cloned by the attacker. For example, an attacker who gains access to the owner's computer might copy a software token. A hardware token might be stolen or duplicated.
- *Something you know* may be disclosed to an attacker. The attacker might guess a password or PIN. Where the token is a shared secret, the attacker could gain access to the CSP or verifier and obtain the secret value. An attacker may install malicious software (e.g., a keyboard logger) to capture this information. Finally, an attacker may determine the secret through off-line attacks on network traffic from an authentication attempt.
- *Something you are* may be replicated. An attacker may obtain a copy of the token owner's fingerprint and construct a replica.

There are several complementary strategies to mitigate these threats:

- *Multiple factors* raise the threshold for successful attacks. If an attacker needs to steal a cryptographic token *and* guess a password, the work factor may be too high.
- *Physical security mechanisms* may be employed to protect a stolen token from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- *Complex passwords* may reduce the likelihood of a successful guessing attack. By requiring use of long passwords that don't appear in common dictionaries, attackers may be forced to try every possible password.
- *System and Network security controls* may be employed to prevent an attacker from gaining access to a system or installing malicious software.

6.2. Token Levels

Password authentication is easy to implement and familiar to users, so many systems rely only on a password for authentication. In this case impersonation of an identity requires

only that the impersonator obtain the password. Moreover, 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. Experience also shows that users are vulnerable to "social engineering" attacks where they are persuaded to reveal their passwords to unknown parties, who are basically "confidence men."

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.

One-time password device tokens are similar to hard tokens. They can be used in conjunction with a password or activated by a password or a biometric to provide multifactor authentication, however one-time password devices do not result in the generation of a shared session authentication key derived from the authentication.

This recommendation requires multifactor authentication for authentication assurance Levels 3 and 4 and assigns tokens to the four levels corresponding to the OMB guidance as follows:

- Password tokens can satisfy the assurance requirements for Levels 1 and 2.
- Soft cryptographic tokens may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3.
- One-time password devices are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3.
- Hard tokens that are activated by a password or biometric can satisfy assurance requirements for Levels 1 through 4.

The above list is a general summary of the assurance levels for tokens. Specific requirements, however, vary with respect to the details of the authentication protocols. Levels 3 and 4 require two-factor authentication. Typically this means that for Level 3 or 4 a password or biometric is used to activate a key. Alternatively, a password protocol may be used in conjunction with a soft token, hard token, or one-time password token to

achieve two-factor authentication. Detailed level by level token requirements are described in conjunction with protocol requirements in Section 8.

7. Registration and Identity Proofing

In the registration process an applicant undergoes identity proofing by a trusted registration authority (RA). If the RA is able to verify the applicant's identity, the CSP registers or gives the applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The applicant is now a subscriber of the CSP and may use the token as a claimant in an authentication protocol.

The RA may be a part of the CSP, or the RA may be a separate and independent entity; however a trusted relationship always exists between the RA and CSP. Either the RA or CSP must maintain records of the registration. The RA and CSP may provide services on behalf of an organization or may provide services to the public. The processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA operates on behalf of an organization, the identity proofing process may be able to leverage a pre-existing relationship (e.g., the applicant is employee or student.) Where the RA provides services to the public, the identity proofing process is generally limited to confirming publicly available information and previously issued credentials.

The registration and identity proofing process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the RA/CSP knows the true identity of the applicant. Specifically, the requirements include measures to ensure that:

1. A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identity a single person;
2. The applicant whose token is registered is in fact the person who is entitled to the identity;
3. The applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the subscriber's token, the subscriber cannot successfully deny he or she registered that token.

An applicant may appear in person to register, or the applicant may register remotely. Somewhat different processes and mechanisms apply to identity proofing in each case. Remote registration is limited to Levels 1 through 3.

7.1. Registration Threats

There are two general categories of threats to the registration process, impersonation and either compromise or malfeasance of the infrastructure (RAs and CSPs). This recommendation concentrates on addressing impersonation threats. Infrastructure threats are addressed by normal computer security controls (e.g., separation of duties, record keeping, independent audits, etc.) and are outside the scope of this document.

7.1.1. Threat Model

While some impostors may attempt to register as any subscriber in the system and other impostors may wish to register as a specific subscriber, registration threats can be categorized as follows:

- Impersonation of a claimed identity – An applicant claims an incorrect identity, supporting the claim with a specific set of attributes created over time or by presenting false credentials.
- Repudiation of registration – A subscriber denies registration, claiming that he/she did not register that token.

7.1.2. Resistance to Registration Threats

Registration fraud can be deterred by making it more difficult to accomplish or increasing the likelihood of detection. This recommendation deals primarily with methods for making impersonation more difficult, however it does prescribe certain methods and procedures that may help to prove who carried out an impersonation. At each level, methods are employed to determine that a person with the claimed identity exists, the applicant is the person who is entitled to that identity and the applicant cannot later repudiate the registration. As the level of assurance increases, the methods employed provide increasing resistance to casual, systematic and insider impersonation.

7.2. Registration 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 the context. 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 CSP shall be prepared to provide records of identity proofing to relying parties as necessary. 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.

If the RA and CSP are remotely located, and communicate over a network, the entire registration transaction between RA and CSP shall be cryptographically authenticated using an authentication protocol that meets the requirements for the assurance level of the registration, and any secrets transmitted shall be encrypted using an Approved encryption method.

The CSP shall be able to uniquely identify each subscriber and the associated tokens and the credentials issued to that subscriber. The CSP shall be capable of conveying this information to verifiers and relying parties. At Level 1, the name associated with the subscriber is provided by the applicant and accepted without verification. At Level 2, the

name associated with the subscriber may be pseudonymous but the RA or CSP must know the actual identity of the subscriber. In addition, pseudonymous Level 2 credentials must be distinguishable from Level 2 credentials that contain meaningful names. At Level 3 and above, the name associated with the subscriber must be meaningful. At all levels, personal identifying information collected as part of the registration process must be protected from unauthorized disclosure or modification.

The following subsection, Section 7.2.1, establishes registration and identity proofing requirements specific to each level. Records retention requirements for each level are specified in Section 7.2.2.

7.2.1. Registration and Identity Proofing Requirements

The following text establishes registration requirements specific to each level. There are no level-specific requirements at Level 1. Both in-person and remote registration are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person registration is permitted at Level 4.

At Level 2 and higher, the applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other individual identifying information. Detailed level-by-level identity proofing requirements are stated in Table 1 below.

Table 1. Identity Proofing Requirements by Assurance Level

	In-Person	Remote
Level 2		
Basis for issuing credentials	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
RA actions	Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	• Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • Address confirmation and notification: a) Sends notice to an address of record confirmed in the records check or; b) Issues credentials in a manner that confirms the address of record supplied by the applicant; or c) Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.
Level 3		
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains applicant's picture and either address of	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number

	In-Person	**Remote**
	record or nationality (e.g. driver's license or passport)	(e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers.
RA actions	Inspects Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then: a) If ID confirms address of record, authorize or issue credentials and send notice to address of record, or; b) If ID does not confirm address of record, issue credentials in a manner that confirms address of record	• Verifies information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. • Address confirmation: a) Issue credentials in a manner that confirms the address of record supplied by the applicant; or b) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.
Level 4		
Basis for issuing credentials	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not Applicable
RA actions	• *Primary Photo ID:* Inspects Photo-ID and verify via the issuing government agency,	Not applicable

	In-Person	Remote
	compare picture to applicant, record ID number, address and DoB. • *Secondary Government ID or financial account* a) Inspects Photo-ID and if apparently valid, compare picture to applicant, record ID number, address and DoB, or; b) Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • *Record Current Biometric* Record a current biometric (e.g. photograph or fingerprints to ensure that applicant cannot repudiate application. • *Confirm Address* Issue credentials in a manner that confirms address of record.	

At Level 2, employers and educational instructors who verify the identity of their employees or students by means comparable to those stated above for Level 2 may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through on-line processes, where notification is via the distribution channels normally used for sensitive, personal communications.

At Level 2, financial institutions subject to the supervision of the Department of Treasury's Office of Comptroller of the Currency may issue credentials to their customers via the mechanisms normally used for on-line banking credentials and may use on-line banking credentials and tokens as Level 2 credentials provided they meet the provisions of Section 8.

In some contexts, agencies may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process. For example, an applicant could be asked to supply non-public information on his or her past dealing with the agency that could help confirm the applicant's identity.

7.2.2. Records Retention Requirements

A record of the facts of registration (including revocation) 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. A minimum record retention period for registration data is:

- For Levels 2, and 3, seven years and six months beyond the expiration, and
- For Level 4, ten years and six months beyond the expiration.

7.3. Mapping FPKI Certificate Policies to Registration Levels

The identity proofing and certificate issuance processes specified in the Federal PKI Certificate Policies [FCBA1, FBCA2, FBCA3] may be mapped to the Registration levels specified in the preceding section. These mappings are as follows:

- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Citizen and Commerce Class policies [FBCA2] are deemed to meet the identity proofing provisions of Level 2.
- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Basic Certificate Policy [FBCA1] are deemed to meet the identity proofing provisions of Levels 2 and 3.
- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Medium, Medium-HW, or High Assurance Certificate policies in [FBCA1] or Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies in [FBCA3] are deemed to meet the identity proofing provisions of Levels 2, 3, and 4.

However, agencies are not limited to relying upon only those certificates by CAs cross-certified with the Federal Bridge CA at Levels 1 and 2. At these levels, 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 7.2.1. At Levels 3 and 4, PKI credentials must be issued by a CA cross-certified[2] with the Federal Bridge CA under one of the certificate policies identified above, or a policy mapped to one of those policies.

[2] Note that bi-directional cross-certification is not required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist.

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 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. Authentication Threats

Threats can be divided into those threats that involve attacks against the actual authentication protocol itself, and other attacks that may reveal either token values, or compromise confidential information. In general, attacks that reveal the token value are worse than attacks that simply compromise some information, because the attacker can then use the token to assume a subscriber's identity.

8.1.1. Authentication Protocol Threats

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 their identity claims could simply be trusted). 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 to test guessed tokens or obtain other information about a specific subscriber;
  - 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 impersonate 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. Because of their ubiquitous use, and the way they are implemented, users of web browser clients are particularly vulnerable to impostor verifiers in password protocols. 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 records and 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. Because of the functional complexity of web browsers, the complexity of their user interfaces, and the control they give servers over what users see, users of web browsers are likely to be vulnerable to password verifier impersonation attacks, even when using or “apparently using” secure protocols (e.g. TLS) that authenticate verifiers;
        - Man-in-the middle attacks where the attacker inserts himself in the path of an authentication exchange, to obtain secret tokens. Because of the functional complexity of web browsers, the complexity of their user interfaces, and the control they give servers over what users see, users of web browsers are likely to be vulnerable to man-in-the-middle attacks on passwords, even when using or “apparently using” secure protocols (e.g. TLS) that are intended to block such attacks;

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 targeted password guessing impractical by requiring use of high-entropy passwords (see Appendix A) and limiting the number of unsuccessful authentication attempts, or by controlling the rate at which attempts can be carried out. To resist untargeted password attacks, a verifier may supplement these controls with network security controls.
- *Replay resistance*: An authentication protocol resists replay attacks if it is impractical to achieve a successful authentication by recording and 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 by generating a per-session shared secret during the authentication process that is subsequently used by the claimant and the relying party 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 token when acting as the verifier. However, even secure protocols can sometimes be bypassed by fooling the claimant into using another protocol or

[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} cryptographic 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.

overriding security controls (for example by accepting unverified server certificates).

- *Man-in-the-middle resistance*: In a man-in-the-middle attack on an authentication protocol, the attacker interposes himself between the claimant and verifier, posing as the verifier to the claimant, and as the claimant to the verifier. The attacker thereby learns the value of the authentication token. Authentication 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 undetected participation of a third party. However, even secure protocols can sometimes be bypassed by fooling the claimant into using another protocol or overriding security controls (for example by accepting unverified server certificates).

8.1.3. Other Threats

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

- Malicious code attacks that may compromise authentication tokens;
- Intrusion attacks that obtain credentials or tokens by penetrating the subscriber/claimant, CSP or verifier system;
- Insider threats that may compromise authentication tokens;
- Out–of-band attacks that obtain tokens in some other manner, such as social engineering to get a subscriber to reveal his password to the attacker, or "shoulder-surfing;"
- Attacks that fool claimants into using an insecure protocol, when they think that they are using a secure protocol, or trick them into overriding security controls (for example, by accepting server certificates that cannot be validated);
- Intentional repudiation by subscribers who deliberately compromise their tokens.

Malicious code could be introduced into the claimant's computer system for the purpose of compromising the claimant's authentication token. The malicious code may be introduced by many means, including the threats detailed below. There are many countermeasures (e.g. virus checkers and firewalls) that can mitigate the risk of malicious code on claimant systems. General good practice to mitigate malicious code threats is outside the scope of this document. Hardware tokens prevent malicious software from extracting and copying the authentication secret token from the token. However, malicious code may still misuse the token, particularly if activation data is presented to the token via the computer. Similarly, the cryptographic tokens at least make it difficult to trick a user into verbally giving away his authentication secret, making social engineering more difficult, while many kinds of passwords are readily expressed over the telephone.

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 10.2 and 10.3 for some helpful references). Note that subscriber/claimant systems are also subject to network intrusion attacks, but appropriate authentication mechanisms are one defense against such attacks.

The most serious consequence of a network intrusion attack is that it might allow an attacker to gain possession or control of tokens used in authentication protocols. 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, due to the constrained environment that holds the keys. Other authentication mechanisms may be vulnerable to an attacker who has access to or can penetrate the claimant's system. However, shared secret mechanisms are potentially subject to penetration attacks against the verifier or CSP as well, where the attacker may find files of many shared secrets. Public key mechanisms are usually less vulnerable to attacks against verifiers or CSPs. Encryption of files containing long-term shared secrets reduces the risks of a successful penetration attack.

Subscribers may intentionally compromise tokens to repudiate authentication. A full discussion of repudiation is outside the scope of this document; typically, however, safeguarding the authentication protocol against other threats will also help to restrict repudiation. A variety of measures will reduce the risk of repudiation, including periodic confirmations that a user has complied with security requirements, confirmations of transactions through a separate channel (such as electronic mail), and reminders to users that delegation of tokens is prohibited. Additional discussion appears in DOJ 2000.

8.2. Authentication Mechanism Requirements

This section covers the mechanical authentication process of a claimant who already has registered a token. Identity proofing and registration are dealt with separately in Section 7. The authentication process shall provide sufficient information to the relying party to

[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.

uniquely identify the registration information provided by the subscriber and verified by the RA in the issuance of the credential.

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 technical requirements for authentication mechanisms (tokens, protocols and security protections) are stated in this section.

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. Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token.

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, password challenge-response protocols that combine a password with a challenge to generate an authentication reply satisfy this requirement although an eavesdropper who intercepts the challenge and reply may be able to conduct a successful off-line dictionary or password exhaustion attack and recover the password. Common protocols that meet Level 1 requirements include APOP [RFC 1939], S/KEY [SKEY], and Kerberos [KERB]. Since an eavesdropper who intercepts such a protocol exchange will often be able to find the password with a straightforward dictionary attack, and this vulnerability is independent of the strength of the operations, there is no requirement at this level to use Approved cryptographic techniques.

At Level 1, long-term shared authentication secrets may be revealed to verifiers.

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.Assertions

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or
- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

8.2.1.3.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. In

addition, any method allowed for the protection of long-term shared secrets at Levels 2, 3 or 4 may be used at Level 1.

8.2.1.4.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^{-10} (1 in 1024), over the life of the password. There are no min-entropy requirements for Level 1. Appendix A contains information about estimating the entropy of passwords.

8.2.1.5.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. Approved cryptography is required to prevent eavesdroppers.

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 valid. Shared secret based authentication systems may simply remove revoked subscribers from the verification database.

CSPs shall revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised to ensure that a claimant using the token cannot successfully be authenticated. If the CSP issues credentials that expire automatically within 72 hours (e.g. issues fresh certificates with a 24 hour validity period each day) then the CSP is not required to provide an explicit mechanism to revoke the credentials. 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.Assertions

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or

- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

Assertions generated by a verifier shall expire after 12 hours and should not be accepted thereafter 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 (including verifiers operated as a part of the CSP), however session (temporary) shared secrets may be provided by the CSP to independent verifiers.

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 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 hashed passwords 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^{-14} (1 in 16,384), over the life of the password. Level 2 passwords shall have at least 10 bits of min-entropy. 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 generally does not adequately block not man-in-the middle attacks or verification impersonation attacks because common web browser clients offer many avenues to fool or trick users. After a successful authentication, 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 cryptographic key using a cryptographic protocol. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token (a secret key or a private key) against compromise by the following protocol threats defined in section 8.1.1: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. Level 3 also requires two factor authentication; in addition to the key, the user must employ a password or biometric to activate the key.

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, or, alternatively shall use a password as well as the key in an authentication protocol with the verifier. If a password is employed to unlock the soft token key, the key shall be kept encrypted under a key derived from a password meeting the requirements for Level 2 authentication, and decrypted only for actual use in authentication. Alternatively, if a password protocol is employed with the verifier, the use of the password shall meet the requirements for Level 2 authentication assurance.

- *Hard token*: a cryptographic key stored on a special hardware device. Tokens must be validated at FIPS 140-2 Level 1 or higher overall. The claimant shall be required to activate the key before using it with a password or biometric, or, alternatively, shall use a password as well as the key in an authentication protocol with the verifier. The authentication mechanism used to authenticate the claimant to unlock token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2. Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance.

- *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 overall. 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 output by the device shall have at least 10^6 possible values. The verifier must be authenticated cryptographically to the claimant, for example using a TLS server. To protect against the use of a stolen token, one of the following measures shall be used:

    - The authentication mechanism used to authenticate the claimant to the token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.

- The claimant sends the verifier a personal password meeting the requirements for (E-authentication) Level 1 with the one-time 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. Approved cryptographic techniques shall be used for all operations.

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 by a key created during the authentication process. Hard token solutions provide the additional assurance of a physical token, and users should know if their token has been stolen. Like soft tokens, hard tokens allow 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 by a key created during the authentication process. One-time password device token systems are commercially available, portable and work easily with any browser client. Like hard tokens, one-time password device tokens 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. Unlike soft tokens or hard tokens, a session key is not created from the authentication process to authenticate subsequent data transfers.

All three token types present the eavesdroppers with similar strong cryptographic protection. Each has its advantages and disadvantages against various 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. Shared secret based authentication systems may simply remove revoked subscribers from the verification database. Verifiers shall check to ensure that the credentials they use are valid.

CSPs shall have a procedure to revoke credentials and 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.

8.2.3.2. Assertions

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or
- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

Assertions generated by a verifier shall expire after 2 hours and should not be accepted thereafter by the relying party.

8.2.3.3.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 algorithms (e.g., AES, SHA-1, SHA256, HMAC) are used for all operations.

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. Level 3 authentication assurance can also be met by tunneling the output of a one-time password device and a Level 1 personal password through a TLS session.

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 only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, 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 or she 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. In addition, the token shall protect the secret from compromise by the malicious code threat as described in section 8.1.3 above. 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, 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. Shared secret based authentication systems may simply remove revoked subscribers from the verification database. 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 8.2.3.3 above.)

8.2.4.3.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.

9. Summary of Technical Requirements by level

This section summarizes the technical requirements for each level in tabular form. Table 2 shows the types of tokens that may be used at each authentication assurance level. Table 3 identifies the protections that are required at each level. Protections are defined in section 8.1.2 above. Table 4 summarizes the requirements for the resistance of passwords to on-line password guessing attacks. Table 5 identifies the types of authentication protocols that are applicable to each assurance level. Table 6 identifies additional required protocol and system properties at each level.

Table 2. Token Types Allowed at Each Assurance Level

Token type	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Table 3. Required Protections

Protect against	**Level 1**	**Level 2**	**Level 3**	**Level 4**
On-line guessing	√	√	√	√
Replay	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking				√

Table 4. Minimum Online Password Guessing Resistance

Attack Type	**Level 1**	**Level 2**
Targeted Attack: Maximum chance of an attacker guessing the password of a selected user over the life of the password with no *a priori* knowledge other than the username	one in 2^{10} (1/1024)	one in 2^{14} (1/16384)
Untargeted Attack: min-entropy	-	10-bits

Table 5. Authentication Protocol Types

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

Table 6. Additional Required Properties

Required Property	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Shared secrets not revealed to third parties by verifiers or CSPs		√	√	√
Multi-factor authentication			√	√
Sensitive data transfer authenticated				√

9.1.1. Relationship of PKI Policies to E-authentication Assurance Levels

Agencies are, in general, issuing certificates under the policies specified in the Common Policy Framework [FBCA3] to satisfy FIPS 201. Table 7 summarizes how certificates issued under these policies correspond to the E-authentication assurance levels. Note that the *Card Authentication* and *Common Device* policies are not listed; these policies support authentication of a system or a cryptographic module rather than a person.

Table 7. E-authentication Assurance Levels and the Common Policy Framework

E-auth Level	Selected Policy Components			Overall Equivalence
	Identity Proofing	**Token**	**Status Reporting**	
Level 2	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies
Level 3	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies
Level 4	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-HW, and Common-High Certificate Policies

Agencies that were early adopters of PKI technology, and organizations outside the Federal government, issue PKI certificates under organization specific policies instead of the Common Policy Framework. The primary mechanism for evaluating the assurance provided by public key certificates issued under organization specific policies is the policy mapping of the Federal Policy Authority to the Federal Bridge CA policies. These policies include the Rudimentary, Basic, Medium, Medium-HW, and High assurance policies specified in [FBCA1] and the Citizen and Commerce class policy specified in [FBCA2]. Table 8 below summarizes how these certificate policies correspond to E-authentication assurance levels. At Level 2 agencies may use certificates issued under policies that have not been mapped by the Federal policy authority, but are

determined to meet the Level 2 identify proofing, token and status reporting requirements.

Table 8. E-authentication Assurance Levels and PKI Certificate Policy Mappings

E-auth Level	Selected Policy Components			Overall Equivalence
	Identity Proofing	**Token**	**Status Reporting**	
Level 2	Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy or other policies that meet level 2 ID proofing requirements	Rudimentary, Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy, any cert with at least 1024-bit RSA key & SHA1 or equivalent.	Basic, Citizen and Commerce Class, Medium, Medium-HW or High Certificate Policy or certs. issued by other CAs with a 72 hour or smaller CRL or revocation cycle	Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy or other policies that meet all level 2 requirements
Level 3	Basic, Medium, Medium-HW, or High Certificate Policy	Rudimentary, Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy	Basic, Medium, Medium-HW, or High Certificate Policy	Basic, Medium, Medium-HW, or High Certificate Policy
Level 4	Medium, Medium-HW, or High Certificate Policy	Medium-HW or High Certificate Policy	Medium, Medium-HW, or High Certificate Policy	Medium-HW or High Certificate Policy

The Federal PKI has also added two policies, Medium Commercial Best practices (Medium-CBP) and Medium Hardware Commercial Best practices (MediumHW-CBP) to support recognition of non-federal PKIs. In terms of e-Authentication levels, the Medium CBP and MediumHW-CBP are equivalent to Medium and Medium-HW, respectively.

10. References

10.1. General References

[DOJ 2000] Guide to Federal Agencies on Implementing Electronic Processes (November 2000), available at: http://www.usdoj.gov/criminal/cybercrime/ecommerce.html

[OCC] Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks. Office of the Comptroller of the Currency, 12 CFR Part 21. May 2003. Available at: http://www.fdic.gov/regulations/laws/federal/03joint326.pdf

[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.

[KERB] Neuman, C., and T. Ts'o, Kerberos: An Authentication Service for Computer Networks, IEEE Communications, vol. 32, no.9, 1994.

[RFC 1939] IETF, RFC 1939, Post Office Protocol - Version 3, May 1996, available at: http://www.ietf.org/rfc/rfc1939.txt

[RFC 2246] IETF, RFC 2246, *The TLS Protocol, Version 1.0*. January 1999, available at: http://www.ietf.org/rfc/rfc2246.txt

[RFC2560] IETF, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, available at: http://www.ietf.org/rfc/rfc2560.txt

[RFC 3280] IETF, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, available at: http://www.ietf.org/rfc/rfc3280.txt

[RFC 3546] IETF, RFC 3546, Transport Layer Security (TLS) Extensions, June 2003, available at: http://www.ietf.org/rfc/rfc3546.txt

[SKEY] IETF, RFC 1760, The S/KEY One Time Password System, February 1995, available at: http://www.ietf.org/rfc/rfc1760.txt

10.2. 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 2002

[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

10.3. 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 800-32] NIST Special Publication, 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 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.

10.4. 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.

10.5. Certificate Policies

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

[FBCA1] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.1 January 12, 2006. Available at http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

[FBCA2] *Citizen & Commerce Certificate Policy*, Version 1.0 December 3, 2002. Available at http://www.cio.gov/fpkipa/documents/citizen_commerce_cpv1.pdf

[FBCA3] *X.509 Certificate Policy for the Common Policy Framework*, Version 2.4 February 15, 2006. Available at http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

Appendix A: Estimating Password Entropy and Strength

Claude Shannon coined the use of the term "entropy[5]" in 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."[6]

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 the attacker 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.

---

[5] 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

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

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 $94^8 \approx 6.09 \times 10^{15}$ – 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

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.

A.2.1 Guessing Entropy Estimate

Guessing entropy is arguably the most critical measure of the strength of a password system, since it largely determines the resistance to targeted, in band password guessing attacks.

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.

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.[7] 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[8].

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

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

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 a 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, and should include at least 50,000 words. 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 of 16 characters or more.
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. The dictionary check requires a dictionary of at least 50,000 legal passwords chosen to exclude commonly selected passwords. Upper case letters in candidate passwords converted to lower case before comparison.

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 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 9^{th} through the 20^{th} 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 both 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 guessing entropy 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.2.2 Min Entropy Estimates

Experience suggests that a significant share of users will choose passwords that are very easily guessed ("password" may be the most commonly selected password, where it is allowed). Suppose, for example, that one user in 1,000 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, who knows the two most commonly chosen passwords can use an automated attack to try those 2 passwords with each user name, and can expect to find at least one password about half the time by trying 700 usernames with those two passwords. 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.

We know of no accurate general way to estimate the actual min-entropy of user chosen passwords, without examining in detail the passwords that users actually select under the rules of the password system, however it is reasonable to argue that testing user chosen passwords against a sizable dictionary of otherwise commonly chosen legal passwords, and disallowing matches, will raise the min entropy of a password. A dictionary test is specified here that is intended to ensure at least 10-bits of min entropy. That test is:

- Upper case letters in passwords are converted to entirely lower case and compared to a dictionary of at least 50,000 commonly selected otherwise legal passwords and rejected if they match any dictionary entry, and
- Passwords that are detectable permutations of the username are not allowed.

This is estimated to ensure at least 10-bits of min entropy. Other means may be substituted to ensure at least 10 bits of min-entropy. User chosen passwords of at least 15 characters are assumed to have at least 10-bits of min-entropy. For example a user might be given a short randomly to character randomly chosen string (two randomly chosen characters from a 94-bit alphabet have about 13 bits of entropy). A password, for example might combine short system selected random elements, to ensure 10-bits of min-entropy, with a longer user-chosen password.

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. Since this is randomly selected password the guessing entropy and min-entropy are both the same value.

It is possible to combine randomly chosen and user chosen elements into a single composite password. For example a user might be given a short randomly selected value to ensure min-entropy to use in combination with a user chosen password string. The random component might be images or a character string.

A.3 Examples

The intent of this guidance is to allow designers and implementers flexibility 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^{-10} (1 in 1024)
2. Level 2 - 2^{-14} (1 in 16,384)

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 $2^{39.5}/2^{14} = 2^{25.5}$ 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 $2^{25.5}$ (about

forty-five 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 limit automated attacks to 3 trials a minute and it would take about 90 years to carryout $2^{25.5}$ trials. If the system required that password authentication attempts be locked for one minute after three unsuccessful trials and that passwords be changed every ten years, then the targeted password guessing attack requirements of Level 2 would be comfortably satisfied. Because the min-entropy of a randomly chosen password is the same as the guessing entropy, the min-entropy requirements of level two are met.

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;
- Used a dictionary to prevent subscribers from including common words and prevented permutations of the username as a password.

Such a password would meet the composition and dictionary rules for user-selected passwords in Appendix A, and from Table A.1 we estimate guessing entropy at 30 bits. Any system that limited a subscriber to less than 2^{16} (about 65,000) failed authentication attempts over the life of the password would satisfy the targeted guessing attack 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 this would easily meet the targeted attack requirements of Level 2. Because of the dictionary test, this would also meet the min-entropy rules for 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 guessing entropy for this password.

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

	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
Length Char.	**No Checks**	**Dictionary Rule**	**Dict. & 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	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

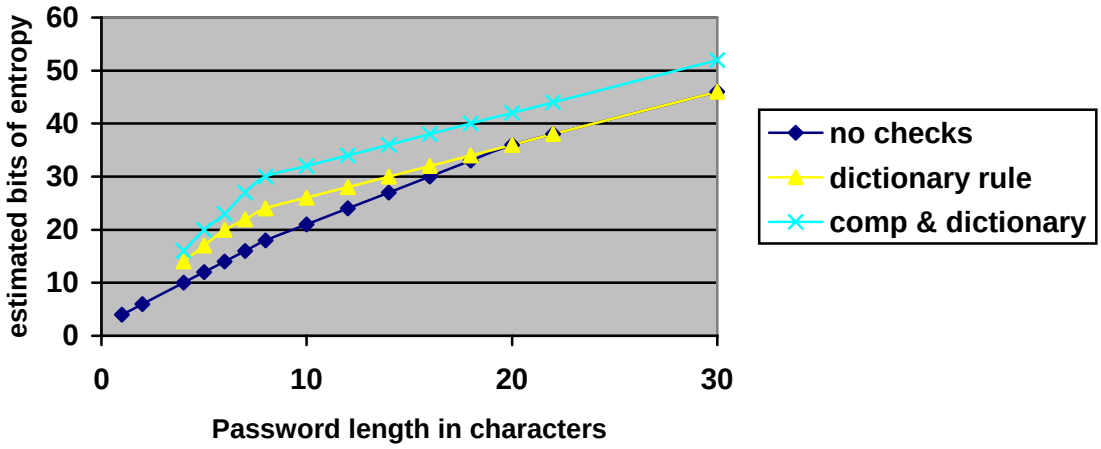

Figure A.1 - Estimated User Selected Password Entropy vs. Length

Appendix B: Errata

Appendix B.1: Errata for Version 1.0.1

1. Cover page: Changed Version number from 1.0 to 1.0.1.
2. Cover page: Changed date from June 2004 to September 2004.
3. Page vii: Clarified text to indicate Level 3 authentication may be supported using one-time passwords, but not reusable passwords.
4. Definition of "Approved" revised to include FIPS 140-2 validation of cryptographic modules and include a URL pointing to the list of validated modules.
5. Page 26: Clarified meaning of "cross-certification" with the Federal Bridge CA by adding a footnote to explicitly state that cross-certification with the Federal Bridge CA need not be bi-directional for the purposes of this guideline.
6. Page 40, Table 2: Clarified that PINS, a form of passwords, are allowed at Levels 1 and 2.

In addition, minor editorial changes (e.g., capitalization, spelling, and punctuation) have been made throughout, and some links have been fixed.

Appendix B.2: Errata for Version 1.0.2

1. Cover page: Changed Version number from 1.0.1 to 1.0.2.
2. Cover page: Changed date from September 2004 to April 2006.
3. Cover page: Specified William Jeffrey as NIST Director and Robert Cresanti as Department of Commerce Under Secretary for Technology
4. Page 25: Updated mapping of FPKI Certificate Policies to 800-63 registration levels to reflect changes in FBCA Basic Assurance Level and incorporate three new FPKI certificate policies (FBCA Medium Hardware policy, Common Authentication, and Common-High). FBCA Basic was upgraded by the Federal PKI Policy Authority to meet Level 3 registration requirements; the new policies satisfy Level 4 Registration requirements.
5. Page 41: A new Table 7 was inserted to clarify the relationship of the certificate policies in the Common Policy Framework with the E-Authentication Assurance Levels. New introductory text associated with this table explains that the Card Authentication and Common Device policies are excluded from consideration, since these policies support authentication of devices.
6. Page 42: Table 8 (Table 7 in version 1.0.1) was updated to reflect the modifications in the Basic certificate policy, which now satisfies Level 3. The new Medium-HW certificate policy, which satisfies Level 4, was also added to this table. Certificate policies from the Common Policy Framework were deleted from this table, since they are specified in the new Table 7.
7. Page 45: URLs for FPKI certificate policies have been updated.