E-Authentication
Password Credential Assessment Profile

Business Owner: Federation Management
Creation Date:
Last Updated: 3/16/05
Version: EA-DD-0013-2.0-F
Audience: Public

Release Notes

PMO Approved

Executive Summary

This document is the Password Credential Assessment Profile (CAP). It is part of the Credential Assessment Portfolio as described in the E-Authentication Credential Assessment Framework (CAF). The reader is assumed to be familiar with the CAF. This document contains criteria used to assess all Password-based Credential Services (CSs) for use in the E-Authentication Initiative. Criteria for Certificate-based CSs are specified by a separate CAP.

Document History

See Appendix C for a detailed list.

Editors

Chris Louden	Judy Spencer	Bill Burr
Kevin Hawkins	David Temoshok	John Cornell
Richard G. Wilsher	Steve Timchak	Stephen Sill
Dave Silver	Von Harrison	

Table of Contents

EXECUTIVE SUMMARY **2**

DOCUMENT HISTORY **3**

EDITORS **3**

TABLE OF CONTENTS **4**

TABLES **4**

1 INTRODUCTION **5**

2 SCOPE **5**

3 TERMINOLOGY **6**

4 CRITERIA **6**

4.1 COMPLIANCE STATUS CODES 6
4.2 SUMMARY OF ASSESSMENT FACTORS 7
4.3 ASSURANCE LEVEL 1 8
4.3.1 Organizational Maturity *8*
4.3.2 Authentication Protocol *9*
4.3.3 Token Strength *12*
4.3.4 Status Management *12*
4.4 ASSURANCE LEVEL 2 13
4.4.1 Organizational Maturity *13*
4.4.2 Registration and Identity Proofing *15*
4.4.3 Authentication Protocol *20*
4.4.4 Token Strength *22*
4.4.5 Status Management *23*
4.4.6 Delivery Confirmation *24*

5 REFERENCES **25**

APPENDIX A GLOSSARY **26**

APPENDIX B ACRONYMS **33**

APPENDIX C DETAILED DOCUMENT HISTORY **34**

Tables

Table 1 Compliance Status Codes 6

1 INTRODUCTION

This document is part of a suite of documents governing the assessment of credentials for use with the E-Authentication Initiative. Please refer to the Credential Assessment Framework (CAF) for an overview. Additional information can be found at **http://www.cio.gov/eauthentication/.**

This Credential Assessment Profile (CAP) contains criteria used to assess Password-based Credential Services (CSs).

2 SCOPE

The scope of the E-Authentication Initiative is 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.

A Password is a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. Passwords encompass Personal Identification Numbers (PINs), which are a special form of password consisting only of decimal digits.

This CAP contains requirements to be met by a Password-based CS to remotely authenticate using a web browser. This CAP **does not** apply to:

- Password-based systems that employ specialized client software for the password authentication protocol;
- Systems that use passwords in conjunction with hard tokens or specialized software;
- Systems where PINs are used in conjunction with physical tokens or specialized software; and
- Other types of CSs (e.g., Certificate-based CS).

The lowest Assurance Level achieved determines the overall authentication Assurance Level. Qualification at any Assurance Level requires validated compliance with all criteria at lower levels of assurance. A full description of the role and scope of the CAP documents is contained in the CAF.

3 TERMINOLOGY

This document relies on terminology defined in NIST Special Publication 800-63, version 1.0.1 '*Recommendations for Electronic Authentication*', and the OMB '*Guidance for E-Authentication*'. See Appendix A, Glossary, for a complete listing of terms used in this context.

4 CRITERIA

The criteria outlined below are organized by credential Assurance Level, and will be applied cumulatively as discussed in Section 2, Scope. Checklists are provided to assist CSs in preparing for an assessment, and to aid the Assessment Team in organizing Assessment findings.

4.1 Compliance Status Codes

Table 1 Compliance Status Codes

Status	Code	Description
Compliant	C	Evidence meets the requirements of the CAF.
Compliance Pending	CP	Evidence indicates that while CSP cannot provide current evidence, it is already in substantial compliance, and is actively working on compliance documentation.
Partial Compliance	P	Evidence indicates that CSP meets some portion of the requirement, but is not actively working on full compliance
Not Compliant	NC	Evidence indicates CSP does not meet the requirement, and is not actively working to become compliant.
Not Applicable	NA	Requirement is not applicable to the CS being Assessed.

4.2 Summary of Assessment Factors

	Level 1	Level 2
Organizational Maturity	☐ Established ☐ Authorization to Operate ☐ General Disclosure	☐ Documentation ☐ Staffing ☐ Subcontracts ☐ Helpdesk ☐ Audit ☐ Risk Mgt ☐ COOP ☐ Logging ☐ Configuration Mgt ☐ Network Security ☐ Physical Security
Registration and Identity Proofing		☐ IVP Disclosure ☐ Records And one or more of: ☐ Confirmed Relationship ☐ In Person Proofing ☐ Remote Proofing
Authentication Protocol	☐ Secure Channel ☐ Proof of Control ☐ Session Authentication ☐ Stored Secrets ☐ Non-repudiation ☐ Threat Protection ☐ Protocol Types ☐ Approved Cryptography ☐ FIPS 140-2	☐ Protected Secrets ☐ Unique ID ☐ Approved Cryptography ☐ Threat Protection ☐ Protocol Types
Token Strength	☐ Uniqueness ☐ Resistance to Guessing ☐ Modifiable	☐ Resistance to Guessing
Status Management	☐ Credential Validity	☐ Credential Status ☐ Credential Revocation
Delivery Confirmation		☐ Confirming Delivery

4.3 Assurance Level 1

4.3.1 Organizational Maturity

Tag	Description	Suggested Evidence of Compliance	Status
Established	1. The CSP shall be a valid legal entity, and a person with legal authority to commit the CSP shall submit the Assessment package. 2. The operational system will be assessed as it stands at the time of the Assessment. Planned upgrades or modifications will not be considered during the assessment.	1. Articles of incorporation, Organizational Charter, Affidavit, etc. 2. Demonstration	
Authorization to Operate	1. The CS shall have completed appropriate authorization to operate (ATO) as required by the CSP policies. 2. The CSP shall demonstrate it understands and complies with any legal requirements incumbent on it in connection to the CS.	1. Copy of ATO or company authorization for Credential Service 2. Asserted in Authorization document as set forth in GSA policies	
General Disclosure	1. The CSP shall make the Terms, Conditions, and Privacy Policy for the CS available to the intended user community. 2. In addition, the CSP shall notify subscribers in a timely and reliable fashion of any changes to the Terms, Conditions, and Privacy Policy.	1. Terms, Conditions, & Privacy policies posted on Website 2. Document how provider will do this.	

4.3.2 Authentication Protocol

Tag	Description	Suggested Evidence of Compliance	Status
Secure Channel	Secrets transmitted across an open network shall be encrypted.	What mechanism is in place to demonstrate this?	
Proof of Control	The authentication protocol shall prove the claimant has control of the authentication password token.	What mechanism is in place to demonstrate this?	
Session Authentication	Session tokens shall be cryptographically authenticated. For example, session cookies must be encrypted, digitally signed, or contain an HMAC.		
Stored Secrets	Secrets such as passwords shall not be stored as plaintext and access to them shall be protected by discretionary access controls that limit access to administrators and applications that require access.	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 an 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. 3. Any method protecting shared secrets at Level 3 or 4 may be used.	

Tag	Description	Suggested Evidence of Compliance	Status
Non-repudiation	Measures shall be taken to reduce the risk of a subscriber intentionally compromising his/her token, to repudiate authentication.	1. Periodic confirmations that a user has complied with security requirements, 2. Confirmations of transactions through a separate channel (such as electronic mail), 3. Reminders to users that delegation of tokens is prohibited.	
Threat Protection	The authentication protocol must resist: 1. On-line guessing 2. Replay	*On-line Guessing* - use CAF Suite's Entropy spreadsheet to show sufficient entropy and min-entropy, as appropriate for assurance level's corresponding token strength requirement. *Replay* - show that it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.	

Tag	Description	Suggested Evidence of Compliance	Status
Protocol Types	The only authentication protocol types allowed at this Assurance Level are: • Tunneled password • Zero knowledge-base password • Challenge-response password	*Tunneled* – show claimant who provides a password through a secure (encrypted) TLS protocol session (tunneling). *Zero knowledge* – show claimant who provides password that does not tell receiver anything about the password the receiver does not already know. *Challenge-response* – show 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.	
Approved Cryptography	1. At this assurance level, cryptographic operations are required between: a) Verifier and Relying Party 2. All cryptographic operations shall be done in compliance with approved cryptographic techniques. 3. Approved cryptographic techniques is either FIPS approved or NIST recommended - an algorithm or technique that is either: 1) Specified in a FIPS or NIST Recommendation, or 2) Adopted in a FIPS or NIST Recommendation.	Assertion is either: 1. Digitally signed by the Verifier; or 2. Obtained directly from the trusted entity (e.g. 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.	
FIPS 140-2	Approved cryptographic algorithms must be implemented in a FIPS 140-2 Level 1 cryptographic module.		

4.3.3 Token Strength

Tag	Description	Suggested Evidence of Compliance	Status
Uniqueness	1. Each subscriber shall self-select at registration time a unique token (e.g., UserID + Password). 2. A user can have more than one token, but a token can only map to one user. 3. Unique tokens cannot be recycled after a subscriber leaves the CS.	What mechanism is in place to ensure uniqueness?	
Resistance to Guessing	At this assurance level, the PIN (numeric-only) or Password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user's PIN or Password shall have a probability of success of less than 2^{-10} (1 chance in 1,024) success over the life of the PIN or Password. Refer to NIST SP 800-63 Appendix A, and the CAF Suites's Entropy Spreadsheet to calculate resistance to online guessing.	1. Demonstrate method of mathematically testing resistance. 2. Use CAF Suite's Entropy Spreadsheet to show sufficient token strength.	
Modifiable	Subscribers must be able to change their passwords	What mechanism is in place to demonstrate this?	

4.3.4 Status Management

Tag	Description	Suggested Evidence of Compliance	Status
Credential Validity	CS shall maintain record of the status of credentials and not authenticate credentials that have been revoked.	What mechanism is in place to demonstrate this?	

4.4 Assurance Level 2

Assessment at Assurance Level 2 also requires validated compliance with all Assurance Level 1 criteria. That is, Assurance Level 2 assessments are cumulative of Assurance Levels 1 and 2.

4.4.1 Organizational Maturity

Tag	Description	Suggested Evidence of Compliance	Status
Documentation	1. The CSP shall have all security related policies and procedures documented that are required to demonstrate compliance. 2. Undocumented practices will not be considered evidence.	Copies or link to policies	
Staffing	1. The CSP shall have sufficient staff to operate the CS according to its policies and procedures. 2. The staff who operate the CS shall have the appropriate skills and abilities for their roles in the operation of the CS.	Roles & Responsibilities defined	
Subcontracts	1. Any subcontractor or outsourced components of the CS shall have reliable and appropriate contractual arrangements, where the agreement stipulates critical policies and practices that affect the assurance of the CS. 2. Subcontractor responsibilities that are not stipulated in their agreements will not be considered reliable during the assessment.	Assert existence of supporting contracts or subcontracts in Authorization document	
Helpdesk	A helpdesk shall be available for subscribers to resolve issues related to their credentials during the CSP's regular business hours, minimally from 9am to 5pm Monday through Friday.	Observe Helpdesk	
Audit	The CSP shall be audited by an independent auditor every 24 months to ensure the organization's practices are consistent with the policies and procedures for the CS. At the time of the assessment, the most recent audit shall have been performed within the last 12 months.	Copy of Latest Audit or Authorization to Operate (ATO).	

Tag	Description	Suggested Evidence of Compliance	Status
Risk Mgt	The CSP shall demonstrate a risk management methodology that adequately identifies and mitigates risks related to the CS.	Copy of Risk Assessment	
COOP	1. The CSP shall have a Continuity of Operations Plan (COOP) that covers disaster recovery and the resilience of the CS. 2. Service level agreements are not assessment criteria; they are covered in the licensing arrangements. 3. The CS shall employ failure techniques to ensure system failures do not result in false positive authentication errors.	1. Review copy of COOP/DR plan 2. Demonstrate	
Logging	The CSP shall log and retain securely for 6 months all significant events related to identity management (e.g., issuance, vetting, and revocation).	Review logs	
Configuration Mgt	The CSP shall demonstrate a Configuration Management methodology that at least includes: 1. Version control for software system components 2. Timely identification and installation of all applicable patches for any software used in the provisioning of the CS.	Review CM logs and documentation	
Network Security	The CSP shall protect their internal communications and systems with measures commensurate with Assurance Level 3 when those communications involve open networks.	Documented protection measures for communications systems.	
Physical Security	The CSP shall employ physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.	Review Physical access, including • Locks • Access lists • Procedures	

4.4.2 Registration and Identity Proofing

Tag	Description	Suggested Evidence of Compliance	Status
IVP Disclosure	1. 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. 2. The practice statement shall address primary objectives of registration and identity proofing, including: • Ensuring a person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person; • Ensuring the applicant whose token is registered is in fact the person who is entitled to the identity • Ensuring 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. 3. Personal identifying information collected as part of the registration process must be protected from unauthorized disclosure or modification. 4. The CSP shall publish its identity verification procedures (IVP) and evidentiary requirements, to the extent necessary to indicate compliance with CAP criteria. That is, the CSP is not de facto required to disclose all of its IVP processes and details. Rather, only enough information to all the Assessment Team to make an informed decision is required.	Review of procedures and requirements	

Tag	Description	Suggested Evidence of Compliance	Status
Records	1. A record of the facts of registration shall be maintained by the CSP or its representative (e.g., Registration Authority). 2. Recording must also include revocation 3. The record of the facts of registration, shall, as a minimum, record: • Full legal name; • Date and place of birth (may not be verified but should be collected); • Current address of record. 4. The minimum record retention period for registration data is seven years and six months beyond the expiration or revocation (whichever is later). 5. 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. 6. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities. 7. At a minimum, credentials shall 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.	Review records and logs	

For each identity proofing mechanism employed by the CSP or RA, one or more of the following three criteria must be met:

Tag	Description	Suggested Evidence of Compliance	Status
Confirmed Relationship	1. The CSP shall know the identity of the applicant for at least one of the following significant purposes: a. Employment b. Government program client c. Banking d. Extension of credit of $2,000 or more e. Issuance of insurance f. Regular payment of bills and a duty of the organization to know the true identity of the applicant g. Matriculation at an accredited degree granting educational institution; h. Compliance with public safety, health or other government regulations that impose a duty to verify the identity or members or participants. 2. The CSP shall confirm that the applicant is a person with a current relationship to the organization, record the nature of that relationship (see above) and certify that the relationship is ongoing and in good standing. 3. Employers and educational instructors who verify the identity of their employees or students by means comparable to those stated for In-person Proofing or Remote Proofing 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. 4. Financial institutions subject to the supervision of the Department	Review sampling of records of ID proofing	

Tag	Description	Suggested Evidence of Compliance	Status
	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 Authentication Protocol requirements.		
In Person Proofing	1. The Registration Authority (RA) shall establish the applicant's identity based on 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) 2. RA inspects photo-ID, compares picture to applicant, records ID number, address and date of birth. 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.	Show Process	
Remote Proofing	1. The RA shall establish the applicant's identity based on 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. 2. RA 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, date of birth, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. 3. Address confirmation and notification:	Show Process	

Tag	Description	Suggested Evidence of Compliance	Status
	a) RA sends notice to an address of record confirmed in the records check or; b) RA issues credentials in a manner that confirms the address of record supplied by the applicant; or c) RA 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.		

4.4.3 Authentication Protocol

Tag	Description	Suggested Evidence of Compliance	Status
Protected Secrets	1. Any secret (e.g., password, PIN, key) involved in authentication shall not be disclosed to third parties by verifier or CSP, with the following exception: • Sharing of session (temporary) shared secrets may be provided to independent verifiers by the CSP. • Sharing of long-term secrets and session secrets with the Agency Application (AA) shall be allowed if no other AA is using the CS. • Long-term secrets and session (temporary) secrets can be shared with infrastructure elements controlled and designated by GSA (e.g., Authentication Service Component).	What mechanism is in place to demonstrate this?	
Unique ID	To support chain of custody capability, a "unique ID" must be used in identity assertions – in accordance with Authentication Service Component interface specifications - that permits recovery of registration records.	Show chain of custody processing, starting with unique ID.	
Approved Cryptography	At this assurance level, cryptographic operations are also required between: a) Claimant and Verifier	What mechanism is in place to demonstrate this?	

Tag	Description	Suggested Evidence of Compliance	Status
Threat Protection	At this assurance level, the authentication protocol must also resist: 1. Eavesdropper	*Eavesdropper* – demonstrate that eavesdropper who records all the messages passing between a claimant and a verifier or relying party finds that it is impractical (see Terminology section) to learn the password or to otherwise obtain information that would allow the eavesdropper to impersonate the claimant.	
Protocol Types	The only authentication protocol types allowed at this Assurance Level are: • Tunneled password • Zero knowledge-base password	*Tunneled* – show claimant who provides a password through a secure (encrypted) TLS protocol session (tunneling). *Zero knowledge* – show claimant who provides password that does not tell receiver anything about the password the receiver does not already know.	

4.4.4 Token Strength

Tag	Description	Suggested Evidence of Compliance	Status
Resistance to Guessing	1. At this assurance level, the PIN (numeric-only) or Password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user's PIN or Password shall have a probability of success of less than 2^{-14} (1 chance in 16,384) over the life of the PIN or Password. 2. The PIN (numeric-only) or Password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker has to guess the most commonly chosen password used in a system) to protect against untargeted attack. Refer to NIST SP 800-63 Appendix A, and the CAF Suite's Entropy Spreadsheet to calculate resistance to online guessing.	1. Demonstrate method of mathematically testing resistance. 2. Use CAF Suite's Entropy Spreadsheet to show sufficient token strength.	

4.4.5 Status Management

Tag	Description	Suggested Evidence of Compliance	Status
Credential Status	CS shall provide, with 99% availability, inclusive of scheduled downtime, a secure automated mechanism to allow the Authentication Service Component (ASC), according to ASC interface specifications, to determine credential status and achieve authentication of the claimant's identity.	Acceptable mechanisms include, but are is not limited to: • Digitally signed revocation list • Status Responder	
Credential Revocation	• The CSP 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.	What mechanism is in place to demonstrate this?	

4.4.6 Delivery Confirmation

Tag	Description	Suggested Evidence of Compliance	Status
Confirming Delivery	The CSP shall issue or renew credentials and tokens in a manner that confirms any one of the applicant's: 1. Postal address of record; OR 2. Fixed-line telephone number of record.	What mechanism is in place to demonstrate this?	

5 REFERENCES

[FIPS-140-2] "Security Requirements For Cryptographic Modules", Federal Information Processing Standard Publication 140-2, 1999.

[M-04-04] The OMB E-Authentication Guidance

[SP 800-63] NIST Special Publication 800-63 version 1.0.1

Appendix A Glossary

Term	Definition
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.
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 a list of validated FIPS 140-2 validated crypto modules see http://csrc.nist.gov/cryptval/.
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.
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.

Term	Definition
Assurance Level	Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.
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.
Bit	A binary digit: 0 or 1.
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	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document uses "credential" broadly, referring to both electronic credentials and tokens.

Term	Definition
Credential Assessment Profile (CAP)	A list of related criteria used to *assess* the Assurance Level of a Credential Service. The E-Authentication Initiative has several CAPs.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential then each one is considered a separate CS.
Credential 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.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]
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.
Cryptographic Module	The set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
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.

Term	Definition
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. Guessing entropy is 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.
FIPS 140-2	Specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The FIPS 140-2 standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.3 d) FIPS 140-2 shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.
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.
Hash-based Message Authentication Code (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.

Term	Definition
Impractical	"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 280 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.
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).
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.
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN.

Term	Definition
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.
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).
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
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.
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 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].
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	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.
Repudiation	Intentional denial of registration (i.e., subscriber claims that he/she did not register that token) or of authentication (i.e., subscriber intentionally compromises his/her token, to repudiate authentication).
Secure Sockets Layer (SSL)	Protocol for transmitting private documents via the Internet by using a private key to encrypt data that's transferred over the SSL connection.

Term	Definition
Session Cookie	Small transient file that contains information about an end user that disappears when the end user's browser is closed. Unlike a persistent cookie, a transient cookie is not stored on an end user's hard drive, but is only stored in temporary memory that is erased when the browser is closed.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier. There are two durations for a shared secret: • Session (temporary) secret – duration of the secret is limited to the duration of the user session. That is, the secret is created, used, and expired during a single user authentication session. • Long-term secret – duration of the secret persists ongoing, and is used from one user authentication session to another user authentication session.
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.
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.
Zero Knowledge password	Claimant who provides password that does not tell receiver anything about the password the receiver does not already know.

Appendix B Acronyms

Acronym	Definition
AA	Agency Application
ANSI	American National Standards Institute
ASC	Authentication Service Component
ATO	Authorization To Operate
CAF	Credential Assessment Framework
CAP	Credential Assessment Profile
COOP	Continuance Of Operations Plan
CS	Credential Service
CSP	Credential Service Provider
DR	Disaster Recovery
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HMAC	Hash-based Message Authentication Code
ID	Identification
IT	Information Technology
IVP	Identity Verification Process
NIST	National Institute Of Standards And technology
OMB	Office Of Management And Budget
PIN	Personal Identification Number
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Socket Layer
TLS	Transport Layer Security

Appendix C Detailed Document History

Status	Release	Date	Comment	Audience
Released	1.0.0	07/10/03	First Release	Limited
Interim	1.3.0	12/19/03	Released for customer review with the proposal that it be accepted for publication as 2.0.0: • §2 - clarification on scope; • §4.2.2 - inclusion of 'secure channel' criteria to comply with revised NIST SP 800-63; • §4.3.1 - amended criteria to comply with revised NIST SP 800-63; • §4.3.2 - revised to remove implied mutual exclusion; • §4.3.2 - revised to reflect requirements of NIST SP 800-63; AND minor proofing amendments which have changed neither the semantics nor the intentions of the document. NB - this document supersedes 1.1.0, which was overtaken by release of the Nov. 2003 draft of NIST SP 800-63 and withdrawn before release.	Customer
Interim	1.4.0	3/1/04	• CP #74 - Consolidate Common, Password and PIN CAPs into a single document – also integrate assessment checklists including "suggested evidence of compliance" and "status" columns. To facilitate integration of Password and PIN CAPS, indicate that PIN is a special form of Password. • Change Name of document to reflect consolidation: Non-PKI CAP , instead of Common CAP	Steve Sill, Sharon Turango, Chris Louden
Draft	1.5.0	1/14/05	• Added Acronyms as Appendix B • Move definitions listing from section 3 to Appendix A because the listing is so long. • Move Executive Summary off the cover page and onto its own page immediately following the cover page. • Use "CAP" throughout, instead of "profile" • CP #1 - Add examples of compliance to authentication protocol types for "Basic Types" tag (§4.3.2), and "Strong Types" tag (§4.4.3), • CP #3 - Add clarification to Scope section (§2) that "The overall authentication assurance level is determined by the lowest assurance level achieved • CP #5 – Add clarification to Scope section (§2) that PIN is a special form of password. • CP #6 - Amend "Credential Revocation" tag (§4.4.5) description to include "The CSP 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" and "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	FSTC Working Group for feedback, via Georgia Marsh

Status	Release	Date	Comment	Audience
			credentials" • CP #8 - Add new tag, "Protocol Types" to Level 1 Authentication Protocol (§4.3.2), and "Protocol Types" to Level 2 Authentication Protocol (§4.4.3). Each describes authentication protocols allowed at that assurance level. • CP #9 - Add new tag "Threat Protection" to Level 1 Authentication Protocol (§4.3.2), and new tag "Threat Protection" to Level 2 Authentication Protocol (§4.4.3). Each describes what threats the authentication protocol must resist, at that assurance level. • CP #10 - Add clarification to "Proof of Possession" tag (§4.3.2), that the authentication token is a password token. • CP #14 - Add to "IVP Disclosure" tag (§4.4.2) the additional requirement that 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 • CP #15 - Add new requirement to "Records" tag (§4.4.2) stating that, at a minimum, credentials shall include identifying information that permits recovery of the records of the registration associated with the credentials… • CP #16 - Add new tag "Unique ID" (§4.4.3) to Authentication Protocol category – to ensure chain of custody capability by working backwards from Unique ID in the assertion, to recover registration record. • CP #17 – Add to "Protected Secrets" tag (§4.4.3)) instruction pertaining to session (temporary) shared secrets, differentiated from long term secret • CP #18 - Add "Approved Cryptography" tag to Level 2. At Level 1, indicate crypto operations are required between Verifier and Relying Party. At Level 2, indicate crypto operations are required between Claimant and Verifier, as well as between Verifier and Relying Party. (§4.3.2, §4.4.3) • CP #18 – Add new tag "FIPS 140-2" indicating that "Approved cryptographic algorithms must be implemented in a FIPS 140-2 Level 1 cryptographic module." (§4.3.2) • CP #18 - Add to "Approved Cryptography" tag (§4.3.2), requirement for FIPS 140-2 validated module. • CP #20 - Amend "Records" tag (§4.4.2) description to include "Either the RA or CSP must maintain records of the registration." Also state that "recording must include revocation" • CP #21 - Added new requirement #2 to "IVP Disclosure" tag (§4.4.2), per NIST SP 800-63, to ensure adherence to primary objectives of registration and identity proofing. • CP #24 – Add to "IVP Disclosure" tag (§4.4.2) "The identity proofing and registration process shall be performed according to a *written policy* or	

Status	Release	Date	Comment	Audience
			practice statement that specifies the particular steps taken to verify identities" • CP # 26 - Add to "IVP Disclosure" tag (§4.4.2) the additional requirement that PII collected as part of the registration process be from unauthorized disclosure or modification. • CP #27 - Revise "In-Person Proofing" tag (§4.4.2) description per NIST SP 800-63 • CP #28 - Revise "Remote Proofing" tag (§4.4.2) description, per NIST SP 800-63 • CP #29 - Add to "Confirmed Relationship" tag (§4.4.2), discussion of employers and educational instructors becoming RA/CSP to issues credentials. • CP #29 - Add to "Confirmed Relationship" tag (§4.4.2), discussion of financial institutions issuing credentials via the mechanisms used for online banking credentials. • CP #30 - Amend "Records" tag (§4.4.2) description to include "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" and "All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities" • CP #31 - Added "Non-repudiation" tag (§4.3.2) to Authentication Protocol category, per NIST SP 800-63, to address a subscriber intentionally compromising token to repudiate the authentication. • CP #33 – added guidance in the "evidence of Compliance" section for "Approved Cryptography" tag indicating assertion must be digitally signed or via a secure authentication protocol. (§4.3.2) • CP #34 - Add examples of evidence to "Credential Status" tag (§4.4.5) • CP #34 - Change wording of "Credential Status" tag (§4.4.5), to be more specific, and to cite more rigorous availability metric (99%) • CP #36 – Add to "Stored Secrets" tag (§4.3.2) clarification as to how secrets must be stored. • CP #40 - Change "Credential Delivery" category name to "Delivery Confirmation". (§4.2,§4.4.6) • CP #43 - Added min-entropy requirement for Strong token strength tag ((§4.4.4) • CP #46 Change Token Strength resistance measures for Basic (§4.3.3) and Strong (§4.4.4) per NIST 800-63. • CP #49 - Add "Password Token" to terminology, per NIST SP 800-63. • CP #49 - Revise and extend terminology section (§3), to align with NIST SP 800-63 terminology, and to provide additional terms as appropriate. • CP #50 - Change "Credential Invalidation" tag to "Credential Revocation" tag (§4.4.5), • CP #50 - Change "Status Responder" to "Credential Status" (§4.4.5) • CP #52 - Delete "as defined in the CAF" from the	

Status	Release	Date	Comment	Audience
			"Proof of Possession" tag (§4.3.2), as terms/concepts will be defined in the Terms section, consistent with NIST SP 800-63. • CP #53 - Rework definition of "Approved Cryptography" tag (§4.3.2), to reflect NIST SP 800-63 definition – FIPS or NIST approved/recommended. • CP #54 - Change "FIPS Crypto" tag (§4.3.2, §4.4.3) to "Approved Cryptography", per NIST SP 800-63 nomenclature. • CP #56 - Delete "Inactivity Expiration" tag from Level 2 Status Management category (§4.4.5) • CP #57 - Delete "Interim" throughout; Do not use "FOC" • CP #58 - Change reference to CAPs, to be "Password" and "Certificate" throughout the document • CP #58 - Use "Password CAP, instead of "Non-PKI CAP" • CP #65 - Add additional requirement to "Uniqueness" tag (§4.3.3): Unique tokens cannot be recycled after a subscriber leaves the CS. • CP #66 - Reference CAF Suite's Entropy Spreadsheet in the Token Strength tags – as a tool to calculate token strength for Basic token strength(§4.3.3), Strong token strength (§4.4.4), Basic Threat Protection (§4.3.2), and Strong Threat Protection (§4.4.3) • CP #74 – delete from Scope section "There may be other requirements for these systems specified by other CAPs.", as it is no longer relevant due to consolidation of Common, Password and PIN CAPS into one CAP – the Password CAP. (§2) • CP #74 – delete from Introduction section "Additional criteria are specified by other CAPs (e.g., Certificate CAP)" because confusing and no longer correct" because, as worded ('additional criteria'), sounds like another CAP has Password criteria, which is no longer the case – even though the intent of the sentence is to indicate that other CAPs exists for other types (e.g., certificate-based) CSs. But this point is made more appropriately in the CAF document, and causes confusion being in this document. (§1) • CP #75 - Change "Credential Status" tag (§4.4.5) and "Protected Secrets" tag (§4.4.3), 3rd bullet to cite current name of "Authentication Service Component", rather than "E-Authentication Service" • CP #80 – change "Proof of Control" tag description to cite 'control' instead of 'possession and control" (§4.3.2) • CP #80 - Change "Proof of Possession" tag name to "Proof of Control" (§4.2, §4.3.2) • CP #82 – Change "Remote Registration" to "Remote Proofing". (§4.2, §4.4.2) • CP #86 - Added scope of E-Authentication as remote electronic authentication of human users….	

Status	Release	Date	Comment	Audience
			(§2) • CP #87, CP#130 - Change token strength tag names "Basic" and "Strong" to "Resistance to Guessing" (although neither change proposal explicitly indicates this name change), so as to be clearer as to what the tag pertains to, and to be consistent with naming conventions used with some newly added tags that appear at multiple levels. (§4.2, §4.3.3, §4.4.4) • CP #89 – In the description for "Established" tag, change "operation" to "operational" (§4.3.1) • CP #90 – change "Identity Proofing" category name to "Registration and Identity Proofing". (§4.2, §4.4.2) • CP #91 – clarify that one or more criteria must be met per identity proofing mechanism. (§4.2, §4.4.2) • CP #107 – In "Evidence of Compliance" column for "Audit" tag, change "IOC" to "Authorization to Operate (ATO)" (§4.4)	
For Approval	1.6.0	1/17/05	• Add References Section (§5)	CEWG
For Approval	1.7.0	2/4/05	• No changes	PMO
PMO Approved	2.0.0	3/16/05	Approved by the PMO	Public