



Office of Information Services  
Centers for Medicare & Medicaid Services  
7500 Security Boulevard  
Baltimore, Maryland 21244-1850

**Standard:**

**CMS Information Security (IS)  
Acceptable Risk Safeguards (ARS)**

**Appendix D**

**CMSR e-Authentication**

**FINAL**  
**Version 4.0**  
**March 19, 2009**

Document Number: CMS-CIO-STD-SEC01-4.0

**(This Page Intentionally Blank)**

**TABLE OF CONTENTS**

**1 INTRODUCTION.....1**

**2 PURPOSE.....1**

**3 E-AUTHENTICATION MODEL .....1**

**4 TECHNICAL REQUIREMENTS BY ASSURANCE LEVEL.....8**

**4.1 Registration and Identity Proofing..... 8**

**4.1 Authentication Mechanism Requirements ..... 12**

    4.1.1 Token ..... 13

**4.1 SUMMARY OF TECHNICAL REQUIREMENTS..... 18**

**LIST OF TABLES**

Table 1 e-Authentication Terms, Abbreviations, and Definitions ..... 3

Table 2 Registration and Identity Proofing..... 8

Table 3 Authentication Mechanism Requirements ..... 13

Table 4 Token Types Allowed at Each Assurance Level ..... 18

Table 5 Required Protections..... 19

Table 6 Authentication Protocol Types ..... 19

Table 7 Additional Required Properties..... 19

**(This Page Intentionally Blank)**

---

## 1 INTRODUCTION

This appendix contains a broad set of CMS standards based upon National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline*, V1.0.2, dated April 2006. It provides technical guidance to CMS to allow an individual person to remotely authenticate his/her identity to a CMS information system.

---

## 2 PURPOSE

Federal Information Systems are required to incorporate information security controls to protect the information systems supporting their operations and missions. CMS is required to ensure the adequate protection of its information assets and must meet a minimum level of information security. NIST SP 800-63 supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] and defines four (4) levels of assurance for electronic transactions, 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. NIST SP 800-63 states specific technical requirements for each of the four (4) levels of assurance.

This document covers remote electronic authentication of human users to CMS information systems over a network. However, 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. Further, this document does not specifically address device-to-device (such as router-to-router) authentication, nor does it establish specific requirements for issuing authentication credentials and tokens to devices and servers when they are used in e-authentication protocols with people.

This document identifies minimum technical requirements for authenticating identity remotely. Business Owners can determine that additional measures are appropriate in certain contexts, based on their risk analysis. In particular, privacy requirements and legal risks may lead Business Owners to determine that additional authentication measures or other process safeguards are appropriate.

---

## 3 E-AUTHENTICATION MODEL

In accordance with OMB guidance [OMB 04-04], e-authentication is the process of establishing confidence in user identities presented electronically to an information system. Systems can use the authenticated identity to determine whether that individual is authorized to perform an electronic transaction. In most cases, the authentications and transactions 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 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 Registration Authority has verified. The token and credential may be used in subsequent authentication events.

In a common case, the Registration Authority and CSP are separate functions of the same system. However, a Registration Authority might be part of an organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral Registration Authority, or it may have relationships with multiple independent Registration Authorities, and a Registration Authority may have relationships with different CSPs as well.

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. Before an applicant can receive credentials or register a token associated with a verified name, he/she must demonstrate that the identity is authentic, and that he/she is the person who is entitled to use that identity. This process is called *identity proofing*, and is performed by a Registration Authority 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 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 summary, first an individual applicant applies to a Registration Authority. The Registration Authority identity proofs that applicant. As the result of successful identity proofing, the applicant becomes a subscriber of a CSP associated with the Registration Authority, with a credential and a secret token registered to the subscriber. When the subscriber needs to authenticate to perform a transaction, he/she becomes a claimant to a verifier. The claimant proves to the verifier that s/he 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. Table 1 provides e-authentication terms, abbreviations and definitions.

**Table 1 e-Authentication Terms, Abbreviations, and Definitions**

Term or Abbreviation	Definitions
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	Party who is not the claimant or verifier but who wishes to execute the authentication protocol successfully as a claimant.
Approved	FIPS approved or NIST recommended. An algorithm or technique that is either: specified in a FIPS or NIST Recommendation; or adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2 (as amended). For more information on validation and a list of validated FIPS 140-2 validated crypto modules see: <a href="http://csrc.nist.gov/cryptval/">http://csrc.nist.gov/cryptval/</a> .
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 quality of data integrity that originates 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 List (CRL)	A list of revoked public key certificates created and signed digitally by a Certification Authority. See [RFC 3280]

Term or Abbreviation	Definitions
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 independently can 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 authenticated himself successfully. 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 as meaning 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 (it requires at least on the order of 279 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 digitally to sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits.
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.

Term or Abbreviation	Definitions
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 a Registration Authority 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 is positioned between the claimant and verifier so that he/she 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. 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, which 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 from 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.

<b>Term or Abbreviation</b>	<b>Definitions</b>
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., Registration Authority, 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 typically is 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 typically is used to verify signatures or encrypt data.
Public Key Certificate	A digital document issued and signed digitally 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 [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 a Registration Authority 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 Registration Authority 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.
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.

Term or Abbreviation	Definitions
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: authenticate the verifier to the claimant; establish an encrypted session between the verifier and claimant; and 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.
Zero Knowledge Password	Strong password used with special "zero knowledge" protocol.
Zero Knowledge Protocol	With Zero-knowledge protocols, someone can convince the verifier that he/she is in possession of the secret without revealing the secret itself, unlike normal username-password queries.

## 4 TECHNICAL REQUIREMENTS BY ASSURANCE LEVEL

### 4.1 REGISTRATION AND IDENTITY PROOFING

In the registration process an applicant undergoes identity proofing by a trusted Registration Authority. If the Registration Authority 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.

Depending on the assurance level, the registration and identity proofing process is designed to ensure that the Registration Authority / CSP know the true identity of the applicant. Specifically, the requirements include measures to ensure that:

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

In some context, Business Owners 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 CMS that could help confirm the applicant’s identity. Table 2 summarizes the registration and identity proofing process.

**Table 2 Registration and Identity Proofing**

Control	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
<b>1. Registration Requirements</b>	There are no level-specific requirements at Level 1.	Both in-person and remote registration are permitted. The applicant must supply his or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS	Both in-person and remote registration are permitted. The applicant must supply his or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS	Only in-person registration is permitted. The applicant must supply his or her full legal name, an address of record, and date of birth, and may also supply other individual identifying information subject to CMS

Control	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
		requirements.	requirements.	requirements.
<b>2. Identity Proofing Requirements</b>				
<b>2.1. Basis for Issuing Credentials (In-Person)</b>	There are no level-specific requirements at Level 1.	Possession of a valid current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality	Possession of verified current primary Government Picture ID (e.g., driver's license or passport) that contains applicant's picture and either address of record or nationality	In-person appearance and verification of two (2) 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 (e.g., driver's license or passport) that contains applicant's picture, and either address of record or nationality, and a new recording of a biometric of the applicant at the time of application.
<b>2.2. Identity Proofing requirements Registration Authority Actions (In-Person)</b>	There are no level-specific requirements at Level 1.	Inspect photo-ID, compare picture to applicant, record ID number, address, and date of birth (DoB). If ID appears valid and photo matches applicant then: 1) If ID confirms address of record, authorize or issue credentials, and send notice to address of record, or; 2) If ID does not confirm address of record, issue credentials in a manner that confirms address of record.	Inspect Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirm 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: 1) If ID confirms address of record, authorize or issue credentials, and send notice to address of record, or; 2) If ID does not confirm	<b>Primary Photo ID:</b> Inspect Photo-ID and verify via the issuing government agency, compare picture to applicant, record ID number, address, and DoB. <b>Secondary Government ID or financial account:</b> 1) Inspect Photo-ID and if apparently valid, compare picture to applicant, record ID number, address, and DoB, or; 2) Verify financial account number supplied by applicant through record checks or through credit bureaus or similar

Control	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
			address of record, issue credentials in a manner that confirms address of record.	databases, and confirm that: name, DoB, address, and other personal information in records that are on balance consistent with the application and sufficient to identify a unique individual.  <b>Record Current Biometric:</b> Record a current biometric (e.g., photograph or fingerprints) to ensure that applicant cannot repudiate application. <b>Confirm Address:</b> Issue credentials in a manner that confirms address of record.
<b>2.3. Basis for Issuing Credentials (Remote)</b>	There are no level-specific requirements at Level 1.	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 <b>either</b> number.	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 <b>both</b> numbers.	<b>Not Applicable</b>
<b>2.4. Registration Authority Actions (Remote)</b>	There are no level-specific requirements at Level 1.	Inspect both ID number and account number supplied by applicant. Verify 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,	Verify 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	<b>Not applicable</b>

Control	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
		and confirms that: name, DoB, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. 1) Address confirmation and notification: 2) Send notice to an address of record confirmed in the records check or; 3) Issue credentials in a manner that confirms the address of record supplied by the applicant; or 4) Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at a number or e-mail address associated with the applicant in records.	information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: 1) Issue credentials in a manner that confirms the address of record supplied by the applicant; or 2) 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.	
<b>3. Records Retention Requirements</b>	There are no level-specific requirements at Level 1.	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 is <b>seven (7) years and six (6) months beyond the expiration or revocation</b> (whichever is later) of the credential.	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 is <b>seven (7) years and six (6) months beyond the expiration or revocation</b> (whichever is later) of the credential.	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 is <b>ten (10) years and six (6) months beyond the expiration or revocation</b> (whichever is later) of the credential.
<b>4. Federal PKI</b>	There are no level-	The identity proofing and	The identity proofing and	The identity proofing and

Control	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
<b>Certificate Policies</b>	<p>specific requirements at Level 1. However, the Public Key Infrastructure (PKI) credentials are not limited to only those certificates by Certification Authorities (CA) cross-certified with the Federal Bridge CA. PKI credentials issued by any CA that has been determined to meet the identity proofing and registration requirements are permitted.</p>	<p>certificate issuance processes of CAs cross-certified with the Federal Bridge CA (FBCA) under policies mapped to the Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level. However, the PKI credentials are not limited to only those certificates by CAs cross-certified with the FBCA. PKI credentials issued by any CA that has been determined to meet the identity proofing and registration requirements are permitted.</p>	<p>certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Basic, Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level. The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies. However, a 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.</p>	<p>certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Medium, Medium-HW, or High Certificate policies are deemed to meet the identity proofing provisions of this level. The PKI credentials must be issued by a CA cross-certified with the FBCA under one of the certificate policies identified above or a policy mapped to one of these policies. However, a 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.</p>

## 4.1 AUTHENTICATION MECHANISM REQUIREMENTS

This section covers the mechanical authentication process of a claimant who already has registered a token. The authentication process shall provide sufficient information to uniquely identify the registration information provided by the subscriber and verified by the Registration Authority in the issuance of the credential. The technical requirements for authentication mechanisms (tokens, protocols and security protections) are described in this section.

### 4.1.1 TOKEN

A token is something that the user possesses and controls (typically a key or password), and used to authenticate the user’s identity. Four (4) kinds of tokens for e-authentication are listed in this section. Each type of token incorporates one or more of the authentication factors (something you know, something you have, or something you are). Tokens that provide a higher level of assurance incorporate two or more factors. Tokens are included which focus upon the protection of critical systems. Unauthorized access frequently results in the compromise of system security and information confidentiality.

This recommendation requires multifactor authentication for e-authentication Assurance Levels 3 and 4, and assigns tokens to the four (4) levels corresponding to the OMB guidance.

**NOTE:** When a control for a system is subject to higher standards to meet specific federal, legal, program, accounting, or other requirements, and the system must be developed to meet these higher standards. This document shall not be construed to relieve or waive these other higher standards.

Table 3 provides a summary of authentication mechanism requirements.

**Table 3 Authentication Mechanism Requirements**

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
<b>1. Tokens</b>	<ul style="list-style-type: none"> <li>On-line guessing</li> <li>Replay</li> </ul>	<ul style="list-style-type: none"> <li>On-line guessing</li> <li>Replay</li> <li>Eavesdropper</li> </ul>	<ul style="list-style-type: none"> <li>On-line guessing</li> <li>Replay</li> <li>Eavesdropper</li> <li>Verifier impersonation</li> <li>Man-in-the-Middle</li> </ul>	<ul style="list-style-type: none"> <li>On-line guessing</li> <li>Replay</li> <li>Eavesdropper</li> <li>Verifier impersonation</li> <li>Man-in-the-Middle</li> <li>Session hijacking</li> </ul>
<b>1.1. Passwords &amp; PINs</b>	Employment of a wide range of available authentication technologies is allowed. The use of any token methods of Levels 2, 3 or 4, as well as passwords is permitted. Common protocols that meet	The use of any of the token methods of Levels 3 or 4, as well as passwords is permitted.	Passwords / PINs may be used as a second level authentication to unlock or use tokens.	Passwords / PINs may be used as a second level authentication to unlock or use tokens.

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
	the requirements include APOP [RFC 1939], S/KEY [SKEY], and Kerberos [KERB].			
<p><b>1.2. One-time Password Device Token</b></p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>If used, One-time Password Device Token shall meet the following requirements:</p> <ul style="list-style-type: none"> <li>• The one-time password output by the device shall have at least 106 possible values.</li> <li>• Passwords must be generated randomly.</li> <li>• The verifier must be authenticated cryptographically to the claimant, for example using a TLS server.</li> <li>• To protect against the use of a stolen token, one of the following measures shall be used:                             <ul style="list-style-type: none"> <li>• 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.</li> <li>• The claimant must send the verifier a personal password meeting the requirements for (e-authentication) Level 1 with the one-time</li> </ul> </li> </ul>	<p><b>Not Applicable</b></p>

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
<p><b>1.3. Software Cryptography Token</b> (A cryptographic key stored on a general-purpose computer.)</p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>password.</p> <p>If used, Software tokens shall meet the following requirements:</p> <ul style="list-style-type: none"> <li>• The user shall be required to activate the key before using a TLS server.</li> <li>• To protect against the use of a password as well as the key in an authentication protocol with the verifier.</li> <li>• If a personal password meeting the requirements for (e-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.</li> </ul>	<p><b>Not Applicable</b></p>
<p><b>1.4. Hardware Cryptography Token</b> (A cryptographic key stored on a special hardware device)</p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>The use of any of the methods of Level 3 is permitted.</p>	<p>If used, Hardware tokens shall meet the following requirements:</p> <ul style="list-style-type: none"> <li>• Tokens must be validated at FIPS 140-2 Level 1 or higher overall.</li> <li>• The user 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.</li> </ul>	<p>Hardware tokens shall meet the following requirements:</p> <ul style="list-style-type: none"> <li>• Token must be validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security.</li> <li>• Requires the entry of a password or a biometric to activate the</li> </ul>

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
			<ul style="list-style-type: none"> <li>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.</li> <li>Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance.</li> </ul>	<p>authentication key.</p> <ul style="list-style-type: none"> <li>Must not be able to export authentication keys.</li> </ul>
<p><b>2. Credential / Token Lifetime, Status or Revocation</b></p>	<p>The use of any of the methods of Levels 3 or 4 is permitted.</p>	<p>The use of any of the methods of Levels 3 or 4 is permitted.</p>	<p>CSPs shall have a procedure to revoke credentials and tokens within one (1) hour.</p>	<p>CSPs shall have a procedure to revoke credentials immediately after being notified that a credential is no longer valid or a token is compromised.</p>
<p><b>3. Assertions</b></p>	<p>Relying parties may accept assertions that are:</p> <ul style="list-style-type: none"> <li>Digitally signed by a trusted entity (e.g., the verifier); or</li> <li>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.</li> </ul>	<p>Relying parties may accept assertions that are:</p> <ul style="list-style-type: none"> <li>Digitally signed by a trusted entity (e.g., the verifier); or</li> <li>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.</li> <li>Assertions generated by a</li> </ul>	<p>Relying parties may accept assertions that are:</p> <ul style="list-style-type: none"> <li>Digitally signed by a trusted entity (e.g., the verifier); or</li> <li>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.</li> <li>Assertions generated by a</li> </ul>	<p>N/A</p>

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
		verifier shall expire after twelve (12) hours and should not be accepted thereafter by the relying party.	verifier shall expire after two (2) hours and should not be accepted thereafter by the relying party.	
<p><b>4. Protection of Long-Term Shared Secrets</b></p>	<p>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.</p>	<p>Long-term shared authentication secrets, if used, shall never be revealed to any party except the subscriber and CSP, however session (temporary) shared secrets may be provided 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 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</p>	<p>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 modules, and is not exported in plaintext from the module. 3) Shared secrets are split by a cryptographic secret</p>	<p>N/A</p>

Controls	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
		hashed passwords are then stored in the password file. 2) Store shared secrets in encrypted form using approved encryption algorithms and modes. Then decrypt the needed secret, when immediately required for authentication. In addition any method protecting shared secrets, at Level 3 or 4 may be used at Level 2.	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).	

## 4.1 SUMMARY OF TECHNICAL REQUIREMENTS

This section summarizes the technical requirements for each level. Table 4 lists the types of tokens that may be used at each assurance level. Table 5 identifies the protections that are required at each level. Table 6 identifies the types of authentication protocols that are applicable to each assurance level. Table 7 identifies additional required protocol and system properties at each level.

**Table 4 Token Types Allowed at Each Assurance Level**

Token Type	Levels of Assurance Level 1	Levels of Assurance Level 2	Levels of Assurance Level 3	Levels of Assurance Level 4
Hard crypto token	X	X	X	X
One-time password device	X	X	X	
Soft crypto token	X	X	X	
Passwords & PINs	X	X		

**Table 5 Required Protections**

<b>Exploits</b>	<b>Levels of Assurance Level 1</b>	<b>Levels of Assurance Level 2</b>	<b>Levels of Assurance Level 3</b>	<b>Levels of Assurance Level 4</b>
On-line guessing	X	X	X	X
Replay	X	X	X	X
Eavesdropper		X	X	X
Verifier impersonation			X	X
Man-in-the-middle			X	X
Session hijacking				X

**Table 6 Authentication Protocol Types**

<b>Prototype Type</b>	<b>Levels of Assurance Level 1</b>	<b>Levels of Assurance Level 2</b>	<b>Levels of Assurance Level 3</b>	<b>Levels of Assurance Level 4</b>
Private Key PoP	X	X	X	X
Symmetric key PoP	X	X	X	X
Tunneled Password or Zero knowledge password	X	X		
Challenge-reply Password	X			

**Table 7 Additional Required Properties**

<b>Required Property</b>	<b>Levels of Assurance Level 1</b>	<b>Levels of Assurance Level 2</b>	<b>Levels of Assurance Level 3</b>	<b>Levels of Assurance Level 4</b>
Shared secrets not revealed to third parties by verifiers or CSPs		X	X	X
Multi-factor authentication			X	X
Sensitive data transfer authenticated				X

**(This Page Intentionally Blank)**