|  |  |
| --- | --- |
| Description: Description: U.S. Department of Health and Human Services Seal | Centers for Medicare & Medicaid Services (CMS) Office of Information Services identity mark. |
| * + - * 1. CENTERS for MEDICARE & MEDICAID SERVICES Enterprise Information Security Group  7500 Security Boulevard Baltimore, Maryland 21244-1850 | |
| E-authentication Workbook  Appendix F :  Level 3 E-Authentication Workbook | |
| *E-authentication Workbook Instructions* | |
| *This workbook contains E-authentication requirements language for use in generating required information necessary to properly generate an SSP. Each workbook must be customized to specifically address the specified system. Specific system data shall be entered in the workbook when a colon symbol is indicated. Enter data to the right of the colon symbol. (Example – System Name: Security CBT). When a table is used, enter the Response Data to the right of or below the subject information under the appropriate table column headings. Delete this cover page prior to completion of this workbook.* | |
| FINAL  Version 1.5  July 31, 2012 | |

(This Page Intentionally Blank)

|  |  |  |
| --- | --- | --- |
| Description: Description: U.S. Department of Health and Human Services Seal | | Centers for Medicare & Medicaid Services (CMS) Office of Information Services identity mark. |
| Office of Information Services Centers for Medicare & Medicaid Services 7500 Security Boulevard Baltimore, Maryland 21244-1850 | | |
| Level 3 E-Authentication Workbook for | | |
| System Name: | | |
| Document Version: |  | |
| Document Date: |  | |
| Template Version 1.5 (FINAL), dated July 31, 2012. | | |

(This Page Intentionally Blank)

Level 3 E-Authentication Workbook

|  |
| --- |
| **Registration and Identity Proofing Control Specification** |
| All applicants will undergo identity proofing by a trusted registration authority. The registration and identity proofing process is designed to ensure that the Registration Authority/CSP know the true identity of the applicant as 1) a person with the applicant’s claimed attributes exists, and those attributes are sufficient to identify a single person uniquely, 2) the applicant whose token is registered is in fact the person who is entitled to the identity and 3) the applicant cannot later repudiate the registration if there is a dispute later about an authentication using the subscriber’s token; the subscriber cannot successfully deny s/he registered that token. |
| **Level 3-1 Registration Policy and Procedures** |
| 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 requirements. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-2 Identity Proofing** |
| **Level 3-2.1 Basis for Issuing Credentials (in-Person)** |
| 1 – Possession of a 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. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-2.2 Registration Authority Action (In-Person)** |
| 1 – Inspect Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| 2.- 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. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| 3.- If ID is valid and photo matches applicant then:  If ID confirms address of record, authorize or issue credentials and send notice to address of record, or;  If ID does not confirm address of record, issue credentials in a manner that confirms address of record. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-2.3 Basis for Issuing Credentials (Remote)** |
| 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 both numbers. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-2.4 Registration Authority Action (Remote)** |
| 1 – 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 information in records are consistent with the application and sufficient to identify a unique individual. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| 2.- Address confirmation and notification:  Issue credentials in a manner that confirms the address of record supplied by the applicant; or  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. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-3 Records Retention Requirements** |
| 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 seven (7) years and six (6) months beyond the expiration or revocation (whichever is later) of the credential. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-4 Federal PKI Certificate Policy** |
| 1 – The identity proofing and certificate issuance processes of CAs cross-certified with the FBCA under policies mapped to the Basic, Medium, Medium-HW, or High Certificate polices 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. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Authentication Mechanism Requirements** |
| Authentication Mechanism Requirements  EA mechanical authentication process covers claimant who already has registered a token. A token is something that the user possesses and control (typically a key or password) and uses to authenticate the user’s identity. The technical requirements for authentication mechanism (tokens, protocols and security protections) are stated in this section. Mechanisms shall be implemented and enforced for all CMS information systems in a manner commensurate with the risk and assurance of the system, network, and data. Supporting procedures shall be developed, documented, and implemented effectively to enable reliable identification of individual users of CMS information systems. |
| **Level 3-5 Tokens Requirements** |
| **Level 3-5.1 Tokens** |
| * On-line guessing * Replay * Eavesdropper * Verifier impersonation * Man-in-the-Middle |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-5.2 Passwords & Pins** |
| 1.- Passwords / PINs may be used as a second level authentication to unlock or use tokens. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-5.3 One-time Password Device Token** |
| 1.- If used, One-time Password Device Token shall meet the following requirements:  The one-time password output by the device shall have at least 106 possible values.  Passwords must be generated randomly.  The verifier must be authenticated cryptographically to the claimant, for example using a TLS server.  To protect against the use of a stolen token, one of the following measures shall be used:  The authentication mechanism used to authenticate the claimant to the token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.  The claimant must send the verifier a personal password meeting the requirements for (E-authentication) Level 1 with the one-time password. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-5.4 Software Cryptography Token (A cryptographic key stored on a general-purpose computer)** |
| 1.- If used, Software tokens shall meet the following requirements:  The user shall be required to activate the key before using a TLS server.  To protect against the use of a password as well as the key in an authentication protocol with the verifier.  If a password is employed to unlock the soft token key, the key shall be kept encrypted under a key derived from a password meeting the requirements for Level 2 authentication, and decrypted only for actual use in authentication. Alternatively, if a password protocol is employed with the verifier, the use of the password shall meet the requirements for Level 2 authentication assurance. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-5.5 Hardware Cryptography Token (A cryptographic key stored on a special hardware device)** |
| 1.- If used, Hardware tokens shall meet the following requirements:  Tokens must be validated at FIPS 140-2 Level 1 or higher overall.  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.  The authentication mechanism used to authenticate the claimant to unlock token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.  Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-6 Credential / Token Lifetime, Status or Revocation** |
| 1.- CSPs shall have a procedure to revoke credentials and tokens within one (1) hour. |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-7 Assertions** |
| 1.- Relying parties may accept assertions that are:  Digitally signed by a trusted entity (e.g., the verifier); or  Obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;  Assertions generated by a verifier shall expire after two (2) hours and should not be accepted thereafter by the relying party |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| **Level 3-8 Protection of Long-Term Shared Secrets** |
| 1.- 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:  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.  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.  Shared secrets are split by a cryptographic secret sharing method between m separate verifier systems, so that the cooperation of n (where 2 ≤ n ≤ 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). |
| **State Compliant or Explain why – Partially Compliant, Non-Compliant or Not Applicable:** |
|  |
| E-authentication Level 1 Security Controls Detail and Comment: |
|  |

**(This Page Intentionally Blank)**