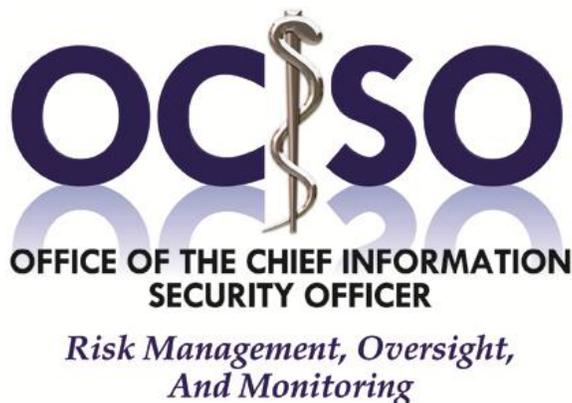




Office of the Chief Information Security Officer
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850



Risk Management Handbook
Volume III
Standard 3.1

CMS Authentication Standards

FINAL
Version 1.1
April 13, 2011

Document Number: CMS-CISO-2011-vIII-std3.1

(This Page Intentionally Blank)

**SUMMARY OF CHANGES IN *CMS AUTHENTICATION STANDARDS*
VERSION 1.1**

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

1 INTRODUCTION.....1

2 AUTHENTICATION COMPONENTS AND MECHANISMS1

2.1 Identity 1

2.2 Credential 1

2.3 Authentication 2

 2.3.1 Multi-factor Authentication 2

3 HUMAN USER AUTHENTICATION3

3.1 Personal Identity Verification (PIV) Cards..... 3

 3.1.1 Homeland Security Presidential Directive 12 3

 3.1.2 To Whom Does HSPD-12 Apply?..... 5

 3.1.2.1 CMS/Federal Employee 5

 3.1.2.2 CMS Contractor 5

 3.1.2.3 Visitor or Temporary 6

 3.1.2.4 Federally Controlled Facilities..... 6

 3.1.2.5 Federally Controlled Information Systems 7

3.2 E-authentication..... 7

 3.2.1 E-authentication Assurance Levels..... 7

 3.2.1.1 E-authentication Level 1 8

 3.2.1.2 E-authentication Level 2 9

 3.2.1.3 E-authentication Level 3 9

 3.2.1.4 E-authentication Level 4 10

 3.2.2 Criteria For Determining E-authentication Levels 10

3.3 Authentication Method Selection Criteria..... 19

3.4 Human Authentication Matrix 21

4 MACHINE-TO-MACHINE AUTHENTICATION23

5 APPROVED23

LIST OF TABLES

Table 1 E-authentication Assurance Level Definitions 8

Table 2 E-authentication Assurance Level Requirements 11

Table 3 Potential Impact Categories and Potential Impact Values 12

Table 4 Maximum Assurance Level for each Potential Impact Category 13

Table 5 CMS Information Types/Levels & E-authentication Level Determination..... 14

Table 6 Human Authentication Matrix 21

(This Page Intentionally Blank)

1 INTRODUCTION

This document provides the Centers for Medicare & Medicaid Services (CMS) position and standard on the use of multi-factor authentication mechanisms in CMS systems.

2 AUTHENTICATION COMPONENTS AND MECHANISMS

2.1 IDENTITY

The information technology world defines *Identity* as the individual characteristics by which a thing or person is recognized or known.

A *digital identity* is the electronic representation of a real-world entity. The term is usually taken to mean the online equivalent of an individual human being, which participates in electronic transactions on behalf of the person in question. Typically known digital identities are established in the form of a UserID. However, a broader definition can also assign digital identities to organizations, companies, and even individual electronic devices.

A digital identity is often used jointly with one or more *credentials* that make (credible) assertions about an entity and a digital identity claimed by the entity.

*In a non-digital application, a **unique credit card number** is a characteristic or **identity** by which a shopper is identified at a store. The **valid** credit card number establishes that certain rights (to purchase on credit) have been established in the name to which the card was issued. The unique credit card number is used by the credit card issuer as the claimed identity of the cardholder. Any **authorized** purchases made under this number will ultimately be linked back to the individual to which the card number was issued.*

2.2 CREDENTIAL

A credential is an attestation of qualification or authority issued to an individual by a *trusted* third party with *authority* to do so. A credential is also an object that is verified when presented to the verifier in an *authentication* transaction. Passwords, digital certificates, tokens, smart cards, mobile phones, or installed software are examples of credentials that may be used for authentication purposes.

*In a non-digital application, a **credential** issued by a **trusted issuer** (such as a government-issued driver's license) is presented by a shopper to a store proprietor in order to establish that the claimed identity (in this case, the credit card number) belongs to the presenter of that identity (the shopper.)*

2.3 AUTHENTICATION

Authentication is the act of establishing or confirming someone (or something) as authentic. Generally this involves *confirming* the identity of a person, tracing the origins of an artifact, and ensuring that an entity (user, process, application, or machine) is what it claims to be. In a digital environment, authentication involves the verification of one or more presented trusted credentials.

In a non-digital application, a store proprietor completes several verifications:

- a. *Verifies the **authenticity of the presented credential** (the driver's license) by checking if the credential has all of the expected attributes provided by the issuer. For the driver's license, the proprietor would verify that the credential is authentic by looking at the State Seal, watermark, or hologram, and checking the expiration date. Since the proprietor has a high confidence in the issuer of the driver's license (the government) and has confidence that the credential is authentic (because the hologram does not appear to be forged, and the license is not expired), they accept the credential as valid.*
- b. *Secondly, the proprietor verifies that the credential presenter (the shopper) is the **authorized** individual to which the credential was issued. This is done by matching the picture on the driver's license with physical attributes of the presenter (the shopper), as observed by the proprietor. If they match, then the presenter is verified as the authorized holder of the credential.*
- c. *Lastly, the proprietor verifies that the **credential matches the identity** provided. If the driver's license name does not match the name on the credit card, then the proprietor cannot establish that the claimed identity (credit card number) belongs to person claiming the identity (the shopper).*

When all three of these verifications are successful, only then can the remainder of the transaction proceed.

2.3.1 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is generally required to access CMS sensitive data. Multi-factor authentication (required as specified in the IA security control family of *CMS Minimum Security Controls [CMSRs]*) uses a combination of two (or more) different methods to authenticate a user identity.

- The first is what users **know**—usually a password, but this can also include a user response to a challenge question. (This is generally known as *Knowledge Based Authentication*, and by itself, is insufficient for authentication to CMS sensitive information.)
- The second is what users **have**. This could be a physical object (token), for example, a smart card, or hardware token that generates one-time-only passwords. It might also be some encrypted software token installed on an individual's system (usually with very limited functional parameters for use.)
- The third is who users **are**, as indicated by some biometric characteristic such as a fingerprint or an iris pattern.

Two-factor authentication means that instead of using only one type of authentication factor, such as only things a user *knows* (passwords, shared secrets, solicited personal information, etc.), a second factor, something the user *has* or something the user *is*, must also be supplied in order to authenticate a user.

Two-factor authentication is not a new concept. Two-factor authentication is used every time a bank customer visits the local ATM. One authentication factor is the physical ATM card the customer slides into the ATM (something they *have*.) The second factor is the PIN they enter (something they *know*.) If the bank customer is without either of these, user authentication cannot take place.

3 HUMAN USER AUTHENTICATION

Human user authentication is the process that provides a level of confidence that the person who is interacting with a system is, in fact, who they claim to be. *Authorization* is the process of enforcing access control policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, the determination of *authorization* occurs within the context of authentication. Once a user is *authenticated*, then they may be determined to be *authorized* for different types of access or activity.

3.1 PERSONAL IDENTITY VERIFICATION (PIV) CARDS

3.1.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12

Homeland Security Presidential Directive 12 (HSPD-12)¹, dated August 27, 2004, entitled *Policy for a Common Identification Standard for Federal Employees and Contractors*, directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors.

The purpose was to create standardized, interoperable *Personal Identity Verification* (PIV) cards, capable of being used as employee and contractor identification, and allowing for both *Physical access*² and *Logical access*³.

It is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees, contractors and subcontractors.

As directed in HSPD-12, the National Institute of Standards and Technology (NIST) Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems.

¹ HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, is available at the US Department of Homeland security at http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

² *Physical Access* means routine, unescorted or unmonitored access to non-public areas of a federally-controlled facility.

³ *Logical Access* means routine, unsupervised, non-public access to a CMS FISMA system.

Federal Information Processing Standard (FIPS) 201⁴, entitled *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005, and amended by Change Notice 1 on June 23, 2006.

FIPS 201 incorporates three NIST Special Publications⁵ specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used.

- NIST Special Publication 800-73, *Interfaces for Personal Identity Verification* specifies the interface and data elements of the PIV card;
- NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification* specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and
- NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

There is *no provision for waivers* to standards issued by the Secretary of Commerce under the Federal Information Security Management Act of 2002 (FISMA). HSPD-12 also has no waiver provision.

On February 3, 2011, the Office of Management and Budget issued OMB Memorandum M-11-11⁶, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, which states the following:

- *Effective immediately*, all new systems under development must use HSPD-12 compliant PIV cards prior to being made operational.
- Starting in fiscal year 2012, existing physical and logical access control systems must be upgraded to use PIV cards prior to the agency using funding for further development or technology refresh.
- All procurements for products and services for facility and system access control must meet HSPD-12 standards and the Federal Acquisition Regulations to ensure interoperability.
- Agencies will accept and electronically verify secure ID cards issued by other agencies.
- Solutions align with and implement the Federal Identity, Credential and Access Roadmap and Implementation Guidance (ICAM).

⁴ FIPS 201 (as amended by Change Notice 1) is available at <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>. (Change Notice 1 provided changes to: 1] the graphics on the back of the PIV card, and 2] the ASN.1 encoding of NACI indicator.)

⁵ All NIST Special Publications are available at <http://csrc.nist.gov/publications/PubsSPs.html>.

⁶ OMB Memorandum M-11-11 is available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>.

3.1.2 TO WHOM DOES HSPD-12 APPLY?

As defined on OMB memorandum M-05-24⁷, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, CMS must conduct a background investigation, adjudicate the results, and issue identity credentials to their *employees* and *contractors* who require long-term (defined as greater than 6-months) *Routine Access*⁸ to Federally controlled facilities and/or information systems.

3.1.2.1 CMS/FEDERAL EMPLOYEE

Which CMS employees need PIV cards?

- Any CMS (Federal) employee, as defined in Title 5 U.S.C § 2105, *Employee*⁹, within a department or agency.
- Other federally employed individuals employed by, detailed to, or assigned to CMS.

Does not apply to:

- Occasional visitors to CMS or contractor facilities to whom you would issue temporary identification.

3.1.2.2 CMS CONTRACTOR

Which contractors need PIV cards?

- Individual under contract or subcontract to CMS, requiring long-term (defined as greater than 6-months) routine access to federally controlled facilities and/or federally controlled information systems.
- Individual under contract or subcontract to CMS requiring any amount of unsupervised logical access. (The PIV credentialing requirements apply whether the contractor accesses the information system from the premises of a CMS facility, from their own facility, through the Internet, or by any other means.)

Does not apply to:

- Contractors who do not need physical or logical access, but need temporary and/or intermittent (supervised) access to CMS facilities or information systems will be treated as visitors and issued alternate credentials. This group includes temporary and seasonal workers, and those needing intermittent physical access such as delivery services.

⁷ OMB Memorandum M-05-24 is available at

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>

⁸ *Routine Access* is defined as regularly scheduled access. For example, a contractor who accesses CMS assets on a regular basis in the performance of ongoing responsibilities has routine access and a personnel investigation must be conducted. A contractor who is summoned for an emergency service call is not required to have a personnel investigation and is treated as a visitor. Contractors who require regularly scheduled access to one or more CMS-controlled assets, even under multiple contracts, should be treated as having routine access.

⁹The definition of "employee" as defined by Title 5 U.S.C § 2105 can be found at <http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t05t08+172+0++%275%20USC%20Sec.%202105%27>

3.1.2.3 VISITOR OR TEMPORARY

Visitors

- Visitor passes are issued for physical access only.
- Visitor passes are issued on the day of use, solely for same-day use.
- Visitor passes expire at the end of the day.

Temporary Credentials

If an employee or long-term contractor forgets his/her card on a particular day, or if the person is waiting for a replacement PIV card, they may be issued a temporary badge after their identity has been confirmed.

At a minimum, the FBI fingerprint check portion of a NACI must be completed prior to issuance of any PIV credential. However, temporary credentials may be issued to new employees and contractors pending the results of the FBI fingerprint check. The temporary credentials will allow limited physical access to CMS facilities and limited logical access to CMS information systems.

3.1.2.4 FEDERALLY CONTROLLED FACILITIES

*Federally Controlled Facilities*¹⁰ are defined as:

- Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency;
- Federally-controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the Directive applies to the 10th floor only;
- Government-owned, contractor-operated facilities, including laboratories engaged in national defense research and production activities; and
- Facilities under a management and operating contract, such as for the operation, maintenance, or support of a Government-owned or Government-controlled research, development, special production, or testing establishment.

The following are *not* Federally Controlled Facilities:

- Contractor owned/contractor operated facilities that provide goods and/or services to CMS under contract.

¹⁰ Pursuant to 48 CFR 2.101 (Title 48, Federal Acquisition Regulations System; Chapter 1, Federal Acquisition Regulation; Subchapter A, General; Part 2, Definitions of Words and Terms; Subpart 2.1, Definitions), available at <https://www.acquisition.gov/far/current/html/Subpart%202.1.html#wp1145507>.

3.1.2.5 FEDERALLY CONTROLLED INFORMATION SYSTEMS

Federally Controlled Information Systems are defined¹¹ as information technology systems (or information systems¹²) used or operated by CMS or by a CMS contractor or other organization on behalf of CMS.

HSPD-12 does not apply to identification associated with *National Security Systems* as defined by FISMA (44 U.S.C. § 3542(2)(A)). *CMS does not currently have systems that qualify under this definition.* Contact the CMS Office of the Chief Information Security Officer (OCISO) at <mailto:ciso@cms.hhs.gov> for questions concerning CMS systems suspected of meeting this definition.

3.2 E-AUTHENTICATION

In accordance with Office of Management and Budget (OMB) Memorandum 04-04, dated December 16, 2003, *E-authentication Guidelines for Federal Agencies*¹³, e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Although not all electronic transactions¹⁴ require authentication, *e-authentication applies to all such transactions for which authentication is required.*

The term *e-authentication* applies to remote authentication of *human users* to Federal agency IT systems for the purposes of conducting government business electronically (or e-government). While authentication typically involves a computer or other electronic device, the term *e-authentication* does **not** apply to the authentication of servers, or other machines and network components.

3.2.1 E-AUTHENTICATION ASSURANCE LEVELS

E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, *Electronic Authentication Guideline*, provides technical guidance (as directed by OMB M-04-04) to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. NIST SP 800-63 addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that they know or possess some secret information.

¹¹ Pursuant to 48 CFR 2.101 (Title 48, Federal Acquisition Regulations System; Chapter 1, Federal Acquisition Regulation; Subchapter A, General; Part 2, Definitions of Words and Terms; Subpart 2.1, Definitions), available at <https://www.acquisition.gov/far/current/html/Subpart%202.1.html#wp1145507>.

¹² In FISMA (44 U.S.C. § 3502(8)) the term *information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

¹³ OMB Memorandum M-04-04 is available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>.

¹⁴ For the purposes of this document, a *transaction* is defined as: a discrete event between user and systems that supports a business or programmatic purpose.

NIST SP 800-63 and OMB M-04-04 define four (4) assurance levels of authentication (i.e., assurance levels 1–4) required by all Federal agencies for electronic government transactions.

The OMB and NIST define the required level of authentication assurance (i.e., e-authentication level) in terms of the likely consequences of an authentication error. Each assurance level describes the degree of certainty that the user has presented an identifier (i.e., a credential¹⁵) that refers to his/her identity. In this context, assurance is defined as: (i) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (ii) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 1 lists the four (4) OMB e-authentication assurance levels and describes their degree of authentication confidence.

Table 1 E-authentication Assurance Level Definitions

| E-authentication Assurance Level | Definition |
|---|--|
| 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. |

3.2.1.1 E-AUTHENTICATION LEVEL 1

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

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

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol. For additional information on the requirements for meeting the e-authentication Level 1 standards, see the *CMS System Security Plan Workbook, Appendix D, Level 1 E-authentication Workbook*, at http://www.cms.gov/informationsecurity/downloads/SSP_Workbook_App_D_L1.zip.

¹⁵ A credential is defined as: an object that is verified when presented to the verifier in an authentication transaction.

3.2.1.2 E-AUTHENTICATION LEVEL 2

Level 2 provides *single factor* remote network authentication. At Level 2, identity-proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider¹⁶ (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol. For additional information on the requirements for meeting the e-authentication Level 2 standards, see the *CMS System Security Plan Workbook, Appendix E, Level 2 E-authentication Workbook*, at http://www.cms.gov/informationsecurity/downloads/SSP_Workbook_App_E_L2.zip.

3.2.1.3 E-AUTHENTICATION LEVEL 3

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

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol. For additional information on the requirements for meeting the e-authentication Level 3 standards, see the *CMS System*

¹⁶ NIST SP 800-63 defines a *Credentials Service Provider* as 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.

Security Plan Workbook, Appendix F, Level 3 E-authentication Workbook, at http://www.cms.gov/informationsecurity/downloads/SSP_Workbook_App_F_L3.zip.

3.2.1.4 E-AUTHENTICATION LEVEL 4

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 e-authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 (*multi-factor*) except that only "hard" cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process. For additional information on the requirements for meeting the e-authentication Level 4 standards, see the *CMS System Security Plan Workbook, Appendix G, Level 4 E-authentication Workbook*, at http://www.cms.gov/informationsecurity/downloads/SSP_Workbook_App_G_L4.zip.

3.2.2 CRITERIA FOR DETERMINING E-AUTHENTICATION LEVELS

Table 2 lists all four (4) e-authentication assurance levels and describes the degree of e-authentication, cryptography, and identity proofing required for each level. As the consequences of an authentication error become more serious, the required level of assurance increases.

Table 2 E-authentication Assurance Level Requirements

| E-authentication Assurance Level | E-authentication Requirement |
|---|--|
| Level 1 | <ul style="list-style-type: none"> ● Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor to provide some assurance that the same claimant (who may be anonymous) is accessing the protected transaction. ● Little or no confidence exists in the asserted identity. ● Cryptography is not required to block offline attacks by an eavesdropper. ● No identity proofing is required. |
| Level 2 | <ul style="list-style-type: none"> ● Requires the claimant prove, through a secure authentication protocol that he or she controls a single authentication factor. ● Confidence exists that the asserted identity is accurate. ● Approved cryptography is required to prevent eavesdroppers. ● Identity proofing procedures require presentation of identifying materials or information. |
| Level 3 | <ul style="list-style-type: none"> ● Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors (i.e., multi-factor). Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens, and "one-time password" device tokens. The claimant must unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two-factor authentication. ● High confidence exists that the asserted identity is accurate. ● Approved cryptography is required for all operations. ● Identity proofing procedures require verification of identifying materials and information. |
| Level 4 | <ul style="list-style-type: none"> ● Requires the claimant prove through a cryptographic protocol that he or she controls a minimum of two authentication factors but only "hard" cryptographic tokens are allowed. ● Very high confidence exists that the asserted identity is accurate. ● Strong, approved cryptographic techniques are used for all operations. ● Requires in-person appearance and identity proofing by verification of two independent ID documents or accounts, one of which must be current primary Government picture ID that contains applicant's picture, and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant. |

The e-authentication assurance level is determined by assessing the potential risks to CMS and by identifying measures to minimize their impact. The risks from an authentication error are a function of two (2) factors: (i) potential harm or impact, and (ii) the likelihood of such harm or impact, as they apply to six (6) OMB-defined potential impact categories. The potential impact for each of the potential impact categories is assessed using the potential impact values described in FIPS 199 (i.e., High, Moderate, or Low).

Table 3 presents the six (6) OMB potential impact categories for authentication errors and their respective potential impact values.

Table 3 Potential Impact Categories and Potential Impact Values

| Level | Potential impact of <i>"inconvenience, distress or damage to standing or reputation"</i> |
|----------|--|
| Low | At worst, limited, short-term inconvenience, distress or embarrassment to any party. |
| Moderate | At worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party. |
| High | Severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals). |

| Level | Potential impact of <i>"financial loss"</i> |
|----------|---|
| Low | At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability. |
| Moderate | At worst, a serious unrecoverable financial loss to any party, or a serious agency liability. |
| High | Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability. |

| Level | Potential impact of <i>"harm to agency programs or public interests"</i> |
|----------|--|
| Low | At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests. |
| Moderate | At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests. |
| High | A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests. |

| Level | Potential impact of <i>"unauthorized release of sensitive information"</i> |
|----------|--|
| Low | At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199. |
| Moderate | At worst, a release of personal, U.S. government-sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199. |

| Level | Potential impact of "unauthorized release of sensitive information" |
|-------|---|
| High | A release of personal, U.S. government-sensitive, or commercially-sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199. |

| Level | Potential impact of "personal safety" |
|----------|--|
| Low | At worst, minor injury not requiring medical treatment. |
| Moderate | At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment. |
| High | A risk of serious injury or death. |

| Level | Potential impact of "civil or criminal violations" |
|----------|---|
| Low | At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts. |
| Moderate | At worst, a risk of civil or criminal violations that may be subject to enforcement efforts. |
| High | A risk of civil or criminal violations that are of special importance to enforcement programs. |

The assurance level is determined by comparing the potential impact category to the potential impact value associated with each assurance level, as shown in Table 4. The required assurance level is determined by locating the highest level whose impact profile meets or exceeds the potential impact for every impact category.

Table 4 Maximum Assurance Level for each Potential Impact Category

| Potential Impact Categories | Assurance Level Impact Profiles | | | |
|---|---------------------------------|-----|-----|----------|
| | 1 | 2 | 3 | 4 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | High |
| Financial loss or agency liability | Low | Mod | Mod | High |
| Harm to agency programs or public interests | N/A | Low | Mod | High |
| Unauthorized release of sensitive information | N/A | Low | Mod | High |
| Personal Safety | N/A | N/A | Low | Mod/High |
| Civil or criminal violations | N/A | Low | Mod | High |

Using the CMS-defined eleven (11) information types¹⁷ and the OMB four (4) e-authentication assurance levels, a determination has been made by the CMS Office of the Chief Information Security Officer (OCISO) as to which assurance level impact profile applied to each potential impact category based on the CMS information type. The results of these determinations are included in Table 5 and published in *CMS System Security and E-authentication Assurance Levels by Information Types*. The basis for determining the overall e-authentication assurance level for each information type is based on selecting the highest applicable impact level for each

¹⁷ CMS Information Types are defined in the *CMS System Security and E-authentication Assurance Levels by Information Type* located at <http://www.cms.gov/informationsecurity/downloads/ssl.pdf>

information type (refer to the bolded, highlighted levels in Table 5). Note that, for the purposes of e-authentication, the authentication requirements apply to users *accessing* the applicable data described. If the system does not (or cannot) present the described information to the user, then that category does not apply, even though the data may exist within the system.

If an individual Business Owner does not agree that the information type processed by their information system requires the same e-authentication authorization level stated in *CMS System Security and E-authentication Assurance Levels by Information Types*, they may use the information provided in Table 5 to demonstrate and explain why the assurance level should be different, and submit an appropriate Risk Acceptance request to the OCISO. The explanation, in accordance with Table 5, and the reasons for modifying the e-authentication assurance level must also be included in the applicable Information System Risk Assessment (IS RA.)

Using the e-authentication assurance level published in *CMS System Security and E-authentication Assurance Levels by Information Types* or the assurance level approved by the CMS CISO, the Business Owner uses Section 4, *Technical Requirements by Assurance Level*, in Appendix D of the *CMS Acceptable Risk Safeguards* to apply the necessary requirements to their information system.

Table 5 CMS Information Types/Levels & E-authentication Level Determination

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|---|---|---|--------------------|------------------------|---------------------|
| Investigation, intelligence-related, and security information (14 CFR PART 191.5(D)) | Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements. | HIGH SC = {(confidentiality, H), (integrity, H), (availability, M)} | | Level 4 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | <Mod> | High |
| | Financial loss or agency liability | Low | Mod | <Mod> | High |
| | Harm to agency programs or public interests | N/A | Low | <Mod> | High |
| | Unauthorized release of sensitive information | N/A | Low | Mod | <High> |
| | Personal safety | N/A | <N/A> | Low | Mod/High |
| Civil or criminal violations | N/A | Low | Mod | <High> | |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|-------------------------------------|--|---|----------|------------------------|----------|
| Mission-critical information | Information and associated infrastructure directly involved in making payments for Medicare Fee-for-Service (FFS), Medicaid and State Children's Health Insurance Program (SCHIP). | HIGH SC = {(confidentiality, H), (integrity, H), (availability, H)} | | Level 4 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | Mod | <High> |
| | Financial loss or agency liability | Low | Mod | <Mod> | High |
| | Harm to agency programs or public interests | N/A | Low | <Mod> | High |
| | Unauthorized release of sensitive information | N/A | Low | Mod | <High> |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | Low | <Mod> | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|----------------------------------|---|---|--------------------|--|----------|
| Information about persons | Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), Equal Employment Opportunity (EEO), personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history as well as personally identifiable information (PII), individually identifiable information (IIF), or personal health information (PHI) covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, M)} | | Case 1: A user can ONLY access or update information about themselves: Level 2 | |
| | | | | Case 2: A user can ONLY submit, review, or update information about persons that THEY have provided DURING THE CURRENT SESSION: Level 2 | |
| | | | | Case 3: A user, not covered in Cases 1 or 2, can access or update information about persons OTHER THAN themselves: Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Case 1 or 2: Mod> | <Case 3: Mod> | High |
| | Financial loss or agency liability | Low | <Case 1 or 2: Mod> | <Case 3: Mod> | High |
| | Harm to agency programs or public interests | N/A | <Case 1 or 2: Low> | <Case 3: Mod> | High |
| | Unauthorized release of sensitive information | N/A | <Case 1 or 2: Low> | <Case 3: Mod> | High |
| Personal safety | <N/A> | N/A | Low | Mod/High | |
| Civil or criminal violations | N/A | <Case 1 or 2: Low> | <Case 3: Mod> | High | |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|---|--|---|----------|------------------------|----------|
| Financial, budgetary, commercial, proprietary and trade secret information | Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included are information about payments, payroll, automated decision making, procurement, market-sensitive, inventory, other financially-related systems, and site operating and security expenditures. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, M)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | <Mod> | High |
| | Financial loss or agency liability | Low | Mod | <Mod> | High |
| | Harm to agency programs or public interests | N/A | Low | <Mod> | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | Low | <Mod> | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|--------------------------------|---|---|----------|------------------------|----------|
| Internal administration | Information related to the internal administration of an agency. Includes personnel rules, bargaining positions, advance information concerning procurement actions, management reporting, etc. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, M)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Mod> | Mod | High |
| | Financial loss or agency liability | Low | <Mod> | Mod | High |
| | Harm to agency programs or public interests | N/A | <Low> | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | <Low> | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|----------------------------------|---|---|----------|------------------------|----------|
| Other Federal agency information | Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, L)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Mod> | Mod | High |
| | Financial loss or agency liability | Low | <Mod> | Mod | High |
| | Harm to agency programs or public interests | N/A | <Low> | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | <Low> | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|---|--|---|----------|------------------------|----------|
| New technology or controlled scientific information | Information related to new technology; scientific information that is prohibited from disclosure or that may require an export license from the Department of State and/or the Department of Commerce. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, L)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Mod> | Mod | High |
| | Financial loss or agency liability | Low | <Mod> | Mod | High |
| | Harm to agency programs or public interests | N/A | <Low> | Mod | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | <Low> | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|-------------------------|--|---|----------|------------------------|----------|
| Operational information | Information that requires protection during operations; usually time-critical information. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, M)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Mod> | Mod | High |
| | Financial loss or agency liability | Low | <Mod> | Mod | High |
| | Harm to agency programs or public interests | N/A | Low | <Mod> | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | <Low> | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|---|--|---|----------|------------------------|----------|
| System configuration management information | Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at an agency; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information. | MODERATE SC = {(confidentiality, M), (integrity, M), (availability, M)} | | Level 3 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | Mod | <Mod> | High |
| | Financial loss or agency liability | Low | Mod | <Mod> | High |
| | Harm to agency programs or public interests | N/A | Low | <Mod> | High |
| | Unauthorized release of sensitive information | N/A | Low | <Mod> | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | Low | <Mod> | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|-----------------------------|---|--|----------|------------------------|----------|
| Other sensitive information | Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare. | LOW SC = {(confidentiality, L), (integrity, L), (availability, L)} | | Level 2 | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | Low | <Mod> | Mod | High |
| | Financial loss or agency liability | Low | <Mod> | Mod | High |
| | Harm to agency programs or public interests | N/A | <Low> | Mod | High |
| | Unauthorized release of sensitive information | N/A | <Low> | Mod | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | N/A | <Low> | Mod | High |

| Information Type | Explanation and Examples | System Security Level | | E-authentication Level | |
|--------------------|--|--|----------|---|----------|
| Public information | Any information that is declared for public consumption by official authorities and has no identified requirement for integrity or availability. This includes information contained in press releases approved by the Office of Public Affairs or other official sources. | LOW SC = {(confidentiality, L), (integrity, L), (availability, L)} | | Case 1: No tracking or control on a user-level basis is desired. Level 0 (No authentication required) | |
| | Potential Impact Categories for Authentication Errors | 1 | 2 | 3 | 4 |
| | Inconvenience, distress or damage to standing or reputation | <Case 1: N/A> <Case 2: Low> | Mod | Mod | High |
| | Financial loss or agency liability | <Case 1: N/A> <Case 2: Low> | Mod | Mod | High |
| | Harm to agency programs or public interests | <N/A> | Low | Mod | High |
| | Unauthorized release of sensitive information | <N/A> | Low | Mod | High |
| | Personal safety | <N/A> | N/A | Low | Mod/High |
| | Civil or criminal violations | <N/A> | Low | Mod | High |

3.3 AUTHENTICATION METHOD SELECTION CRITERIA

All CMS *Human User* authentication requirements (this section does *not* apply to *Machine-to-Machine* authentication) are stipulated in the *CMS Information Security Acceptable Risk*

Safeguards (ARS), *CMS Minimum Security Requirements (CMSR)* manual¹⁸, in the *Identification and Authentication (IA)* family of security controls. The primary factor for determining which type of authentication is required is the *population of users* that will be accessing the information system. NIST has segregated¹⁹ the users into two populations; *Organizational* and, *Non-Organizational*, and addresses the applicable authentication requirements in two separate and distinct control requirements. CMS defines these user populations as follows:

- **Organizational Users** - Organizational users are defined as personnel who are accessing a CMS system (whether that system is hosted by CMS, or hosted by a CMS contractor) for the purposes of performing duties associated with their CMS employment or contractual relationship with CMS. Organizational user-authentication requirements are stipulated in IA-2 and its enhancements (enhancement applicability is dependent on the system security level.) **For organizational users, e-authentication requirements of Section 3.2 are superseded by the requirements listed in IA-2.** Organizational users include (but are not limited to):
 - CMS employees
 - CMS contractor/subcontractor staff
 - CMS-contracted researchers
- **Non-Organizational Users** - Non-organizational users are defined as users that are accessing CMS systems for any other purpose other than those defined in the definition of *Organizational users*. **Non-organizational user-authentication requirements are stipulated in IA-8, and are solely based on the applicable e-authentication level of Section 3.2.** These users include (but are not limited to):
 - Beneficiaries
 - Providers
 - State Medicaid employees and contractors/subcontractors
 - Non CMS-contracted researchers

Other factors that influence the CMS level of authentication requirement include:

- **The Level of Access of the user** - At CMS, *privileged access* is defined as an advanced level of access to a computer or application that includes the ability to perform configuration changes (to either the application or the underlying supporting infrastructure.) Some applications may have users with more *functionalities* than the normal user population; however, that does not necessarily mean that they would be considered *privileged* users. Users with *privileged* access rights require more stringent authentication than those users accessing via *non-privileged* account roles. Users with *privileged* access rights would be considered *organizational* users (and would be subject the requirements stipulated in IA-2.)
- **Access Method used to connect to the system** - CMS Access methods are segregated into three distinct types:

¹⁸ The ARS manual can be found at <http://www.cms.gov/InformationSecurity>.

¹⁹ These distinctions are made in the IA family of controls enumerated in the NIST SP 800-53, from which the ARS manual, and its associated control requirements, are directly derived.

- *Local access* - Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network.
- *Trusted Network access* is defined as the ability to *authenticate* to a CMS computer or network via a connection through a *trusted data link*.
- *Untrusted Network access* is defined as the ability to *authenticate* to a CMS computer or network via a connection through an *untrusted data link*.

The Trustworthiness of the data link - The trustworthiness of CMS data links is segregated into two distinct types:

- A *Trusted data link* is defined as a data-link that can be relied upon to enforce CMS security policy and security control requirements (as verified in a CMS system ATO.) Examples include (but are not limited to):
 - Internal CMS LAN
 - An *established* encrypted VPN that meets all applicable CMS security requirements. (See *Machine-To-Machine Authentication* requirements in Section 4.)
- An *Untrusted data link* is defined as a data-link that cannot be relied upon to enforce CMS security policy and security control requirements. Examples might include (but are not limited to):
 - The Internet
 - Any network not included in a CMS FISMA system.
 - Networks included in a CMS FISMA system, but identified as non-compliant with CMS security requirements.

3.4 HUMAN AUTHENTICATION MATRIX

Table 6 provides a *high-level* matrix for human authentication requirements under the various conditions described above. Note that for *non-organizational/non-privileged* users covered under e-authentication requirements (as defined in Section 3.3); a further evaluation must still be performed to determine the applicable e-authentication Level (1, 2, 3, or 4) and the associated requirements thereof.

Table 6 Human Authentication Matrix

| System Security Level (Defined in Table 5) | User Role (Defined in Section 3.3) | User Type (Defined in Section 3.3) | Access Method (Defined in Section 3.3) | Authentication Required (Defined in Section 2.3.1) |
|---|---------------------------------------|---------------------------------------|---|---|
| Low | Non-Privileged | Organizational | Local | Single-factor |
| Low | Non-Privileged | Organizational | Trusted Network | Single-factor |
| Low | Non-Privileged | Organizational | Untrusted Network | Single-factor |
| Low | Non-Privileged | Non-Organizational | Local | Single-factor |

| System Security Level (Defined in Table 5) | User Role (Defined in Section 3.3) | User Type (Defined in Section 3.3) | Access Method (Defined in Section 3.3) | Authentication Required (Defined in Section 2.3.1) |
|---|---------------------------------------|---------------------------------------|---|---|
| Low | Non-Privileged | Non-Organizational | Trusted Network | Single-factor |
| Low | Non-Privileged | Non-Organizational | Untrusted Network | Single-factor |
| Low | Privileged | Organizational | Local | Multi-factor |
| Low | Privileged | Organizational | Trusted Network | Multi-factor |
| Low | Privileged | Organizational | Untrusted Network | Multi-factor |
| Low | Privileged | Non-Organizational | < Any > | < Not allowed > ²⁰ |
| Moderate | Non-Privileged | Organizational | Local | Single-factor ²¹ |
| Moderate | Non-Privileged | Organizational | Trusted Network | Single-factor ²¹ |
| Moderate | Non-Privileged | Organizational | Untrusted Network | Multi-factor |
| Moderate | Non-Privileged | Non-Organizational | Local | Multi-factor ²² |
| Moderate | Non-Privileged | Non-Organizational | Trusted Network | Multi-factor ²² |
| Moderate | Non-Privileged | Non-Organizational | Untrusted Network | Multi-factor ²² |
| Moderate | Privileged | Organizational | Local | Multi-factor |
| Moderate | Privileged | Organizational | Trusted Network | Multi-factor |
| Moderate | Privileged | Organizational | Untrusted Network | Multi-factor |
| Moderate | Privileged | Non-Organizational | < Any > | < Not allowed > |
| High | Non-Privileged | Organizational | Local | Single-factor ²¹ |
| High | Non-Privileged | Organizational | Trusted Network | Single-factor ²¹ |
| High | Non-Privileged | Organizational | Untrusted Network | Multi-factor |
| High | Non-Privileged | Non-Organizational | Local | Multi-factor |
| High | Non-Privileged | Non-Organizational | Trusted Network | Multi-factor |
| High | Non-Privileged | Non-Organizational | Untrusted Network | Multi-factor |
| High | Privileged | Organizational | Local | Multi-factor |
| High | Privileged | Organizational | Trusted Network | Multi-factor |
| High | Privileged | Organizational | Untrusted Network | Multi-factor |
| High | Privileged | Non-Organizational | < Any > | < Not allowed > |

²⁰ Privileged access for non-organizational users is not allowed. All users requiring privileged access are treated as organizational users.

²¹ The CMS CIO has reduced these requirements (temporarily) from Multifactor to Username/Password due to the high cost-impact for implementation on the entire CMS enterprise. However, it should be noted that this is **not compliant** with FIPS 200 (and SP 800-53) nor OMB M-11-11 requirements and will be elevated to a compliant Multifactor requirement in the **next release** of the CMS Information Security Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirements (CMSR). Newly-developed systems should endeavor to integrate multifactor solutions where feasible to lower retrofit costs in the future.

²² May only require E-authentication Level 2 if applicable conditions for PII/PHI (user can only see information about themselves), and no other Moderate-level information is present. See Table 5 for details.

4 MACHINE-TO-MACHINE AUTHENTICATION

This section is under development and will be included in a future update to this standard.

5 APPROVED

C. Ryan Brewer
CMS Chief Information Security Officer and
Director, Office of the Chief Information Security Officer

This document will be reviewed periodically, but no less than annually, by the Office of the Chief Information Security Officer (OCISO), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the OCISO at <mailto:ciso@cms.hhs.gov>.

(This Page Intentionally Blank)