# DoD Instruction 8520.03

# Identity Authentication for Information Systems

| | |
|---|---|
| **Originating Component:** | Office of the DoD Chief Information Officer |
| **Effective:** | May 19, 2023 |
| **Releasability:** | Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/. |
| **Reissues and Cancels:** | DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, as amended |
| **Incorporates and Cancels:** | See Paragraph 1.3. |
| **Approved by:** | John B. Sherman, DoD Chief Information Officer |

**Purpose:** In accordance with the authority in DoD Directive 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and provides procedures for authenticating person and non-person entities (NPEs) to DoD information systems, including credential management.
- Establishes policy and prescribes procedures for establishing credentials and performing identity authentication of all entities accessing DoD information systems that authenticate themselves to DoD or external entities in accordance with DoD Instruction (DoDI) 8500.01.
- Establishes sensitivity levels to align with risk management requirements as specified in DoDI 8510.01, and establishes credential strengths to better align with identity proofing, credential management, and authentication requirements as specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3.
- Implements use of hardware public key infrastructure (PKI) certificates such as the personal identity verification (PIV) authentication public key certificate, as defined in the NIST Federal Information Processing Standard (FIPS) 201-2, on the DoD common access card (CAC), as the preferred authenticator for person entities to use when accessing DoD information systems on unclassified networks.
- Provides guidance on using authenticators including hardware and software PKI based, username and password, multi-factor authentication (MFA), and assertions.

# TABLE OF CONTENTS

# SECTION 1: GENERAL ISSUANCE INFORMATION

## 1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD (referred to collectively in this issuance as the "DoD Components").

(2) The U.S. Coast Guard for Coast Guard-operated DoD systems and networks and for Coast Guard information systems and networks that directly affect the Department of Defense Information Network (DODIN) and DoD mission assurance in accordance with the January 17, 2017 Memorandum of Agreement between DoD and the Department of Homeland Security Regarding DoD and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations.

(3) All DoD Unclassified, Secret, and U.S.-owned networks and information systems under the authority of the Secretary of Defense (e.g., Non-classified Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET), Defense Research and Engineering Network, Secret Defense Research and Engineering Network, SIPRNET Releasable, De-Militarized Zone, United States Battlefield Information Collection and Exploitation System, and other DoD Mission Partner Environments). Information systems include those that are owned and operated by, or on behalf of, DoD, including systems hosted at DoD data centers, contractor-operated systems processing DoD owned information, cloud hosted systems including platform as a service and infrastructure as a service, and systems hosted on closed operational networks with no connection to the DODIN.

(4) DoD Components using third-party software as a service commercial systems when used to authenticate users for access to DoD resources.

(5) Information systems supporting physical access control to DoD facilities.

(6) DoD Components granting access to DoD and non-DoD entities including person entities and NPE (e.g., physical devices, virtual machines, information systems, robotic process automation (RPA) and artificial intelligence bots, and other processes) logically accessing DoD Unclassified, Secret, and information systems under the authority of the Secretary of Defense, including DoD mission partners and DoD beneficiaries.

b. This issuance does **not** apply to:

(1) Information systems processing, storing, or transmitting sensitive compartmented information under the existing authorities and policies of the Director of National Intelligence as directed by Executive Order 12333 and other applicable laws and regulations.

(2) Information systems operated by the DoD Special Access Program (SAP) community. Due to the highly sensitive nature of SAPs and their materials, these systems must be managed independently and fall under the purview of the DoD SAP Chief Information Officer (CIO). For additional details regarding SAP requirements, please contact the DoD SAP CIO office.

## 1.2. POLICY.

a. Information system owners must evaluate risks to determine and document the requirements for authentication for the overall information system in accordance with DoDI 8510.01. In addition, information system owners must evaluate risk for specific resources hosted by the information system, and for functional and information technology (IT) privileged user roles within the information system based on this issuance.

b. Information systems must authenticate all entities using approved credentials as described in Section 3 before granting access to information or other resources. Information systems that cannot meet the requirements in Section 3 must obtain a temporary exception to policy (E2P) as described in Section 4. Information approved for public release in accordance with DoDIs 5230.09 and 5230.29 does not require authentication to access.

(1) DoDI 8520.02 defines the DoD PKI and provides the approval process for external PKI Credential Service Providers (CSP). Public key certificates issued by PKIs approved in accordance with DoDI 8520.02 are approved for authentication as described in Section 3.

(2) Authentication based on DoD approved PKI is preferred for all use cases. Authentication based on alternative MFA or single-factor authentication such as username and password is only approved as described in Section 3. DoD-approved MFA is preferred over single-factor authentication and used, when possible, even when single factor authentication is permitted.

(3) An identity provider (IdP) authentication service may be used to perform authentication and provide an assertion to the information system when:

(a) The IdP meets the requirements in Paragraph 3.6., which are designed to prevent the unauthorized generation or modification of assertions.

(b) The IdP is either a reverse proxy IdP or is approved as a general purpose IdP in accordance with Paragraph 4.2.

(c) The IdP can only generate assertions that are at or below the protections it is operating with for its own assertion signature key as defined in NIST SP 800-63-3. For example, an IdP that protects its signing key in software that is operated at an Authenticator Assurance Level (AAL) 2, and can only assert AAL1 or AAL2, even if the original authenticator used an AAL3 credential.

(d) The information system can determine that the original entity authentication to the IdP met the authentication requirements for the information system use case as described in Section 3. This determination can be made where the IdP:

1. Only supports a single type of authenticator;

2. Includes information on the original authentication method in the assertion; or

3. Incorporates rules such that it only creates assertions where the original authentication method is sufficient for the resource being requested.

(4) Organizations that manage information systems that have connectivity to the DODIN or commercial Internet must not require authorized entities to obtain a new credential solely for the purpose of logical access if the entity possesses a public key certificate issued by a DoD-approved PKI. Information systems that are approved for MFA or single-factor authentication in accordance with Section 3 may also support alternate authenticators if needed to accommodate access from workstations, mobile devices, or other endpoints that do not support PKI-based authentication or are not DoD or mission partner owned and managed.

c. Information system owners must use DoD enterprise identity, credential, and access management (ICAM) solutions when enterprise solutions address information system ICAM needs. As DoD enterprise ICAM solutions mature, information system owners must re-evaluate decisions to use locally managed solutions and transition to DoD enterprise ICAM solutions to the maximum extent possible.

## 1.3. CANCELLED DOCUMENTS.

This issuance incorporates and cancels the following DoD CIO memoranda:

a. "Assignment of Program Integration Office Responsibilities for the Department of Defense Identity, Credential and Access Management Program," January 3, 2020.

b. "Department of Defense Requirements for Accepting Non-Federally Issued Identity Credentials," January 24, 2013.

c. "DoD SIPRNet Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNet Applications and Web Servers," October 14, 2011.

d. "Exceptions to DoD Classified Network Public Key Infrastructure Hardware Token Logon Requirements," April 21, 2014.

e. "Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication," July 5, 2015.

f. "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems," August 20, 2018.

g. "Modernizing the Common Access Card – Streamlining Identity and Improving Operational Interoperability," December 7, 2018.

# SECTION 2: RESPONSIBILITIES

## 2.1. DOD CIO.

In addition to the responsibilities in Paragraph 2.8., the DoD CIO:

a. Approves:

(1) MFA technologies for use by DoD information systems.

(2) General purpose IdPs for use by DoD information systems.

(3) E2P for DoD information systems that are unable to meet the identity and authentication requirements in this issuance.

b. Serves as DoD's joint lead for identity management activities with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), pursuant to DoDIs 1000.25 and 1000.13.

c. Chairs the Identity Protection and Management Senior Coordinating Group, in accordance with DoDI 1000.25, which provides overall ICAM direction and leadership for DoD, including adjudicating ICAM implementation decisions that cross DoD Component boundaries and addressing funding, resources, and other barriers to ICAM implementation.

d. Supports meetings of governmental and commercial ICAM working groups and organizations.

e. Coordinates with:

(1) The Under Secretary of Defense for Intelligence and Security (USD(I&S)) and USD(P&R) on the needs of DoD for identity proofing, identity resolution, credential management, and authentication.

(2) DoD Components and the ICAM Joint Program Integration Office (JPIO) for requirements definition and program oversight for enterprise ICAM services that support identity, credential, and authentication activities.

f. Oversees integration with the cybersecurity risk management framework as defined in DoDI 8510.01 and NIST SP 800-63-3.

g. Provides guidance to facilitate implementing identity, credential, and authentication processes and procedures, including maintaining the ICAM Reference Design.

h. Designates an individual to serve as the DoD CIO ICAM lead to support coordination, including approval requests for MFA technologies and IdPs operated externally to DoD.

i. Maintains a list of approved MFA technologies and approved IdPs in a format that is accessible to DoD information system owners.

## 2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.8., the Director, DISA:

a. Provides a senior executive-level individual to lead the ICAM JPIO, provides action officer level coordination across ICAM JPIO member organizations, and coordinates DISA operated enterprise ICAM services. Through the ICAM JPIO lead or deputy leads, the Director, DISA:

(1) Ensures that DoD enterprise ICAM services operated by the National Security Agency (NSA), DISA, and Defense Manpower Data Center (DMDC) meet the needs of DoD, interoperate with each other, and support interoperability with ICAM services operated by the DoD Components.

(2) Develops and maintains a DoD Enterprise ICAM Service Implementation Plan to support the DoD ICAM Strategy.

b. Establishes, operates, tests, and maintains enterprise ICAM services that support identity, credential, and authentication activities including the DoD PKI, an IdP with MFA service, automated account provisioning service, and master user record service.

c. Provides cybersecurity services for DISA-operated enterprise ICAM services in accordance with DoDI 8530.01.

d. Establishes, operates, and maintains a capability for testing the interoperability of DoD Component, community of interest (COI), and external IdPs with DoD information systems.

e. Coordinates with the Director, NSA to develop and maintain security requirements guides (SRG) and security technical implementation guides for products and services that support identity, credentialing, and authentication, including approved MFA technologies and IdP products, incorporating National Information Assurance Partnership (NIAP) validation when applicable.

f. Provides subject matter expertise and technical support to DoD Components for implementing authentication capabilities and integration with DISA-operated enterprise ICAM services.

## 2.3. USD(I&S).

In addition to the responsibilities in Paragraph 2.8., the USD(I&S) coordinates with the DoD CIO and USD(P&R) on the needs of DoD for identity proofing, identity resolution, credential management, and authentication.

## 2.4. DIRECTOR, NSA/CHIEF CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.8., the Director, NSA/Chief, Central Security Service, in coordination with the DoD Chief Information Security Officer (CISO):

a. Provides a senior executive-level individual to serve as a deputy lead for the ICAM JPIO and to coordinate DoD enterprise ICAM services operated by NSA. Through the ICAM JPIO lead or deputy leads, the Director, NSA/Chief, Central Security Service:

(1) Ensures that DoD enterprise ICAM services operated by the NSA, DISA, and DMDC meet the needs of DoD, interoperate with each other, and support interoperability with ICAM services operated by the DoD Components.

(2) Develops and maintains a DoD Enterprise ICAM Service Implementation Plan to support the DoD ICAM Strategy.

b. Coordinates with DISA to develop and maintain SRGs and security technical implementation guides for products and services that support identity, credentialing, and authentication, including approved MFA technologies and IdP products, incorporating NIAP validation where applicable.

c. Supports DoD enterprise ICAM services to address DoD mission requirements through research and development and technical and security guidance to DoD enterprise ICAM service providers.

d. Provides systems engineering support and testing support, including threat assessments, for DoD enterprise ICAM services.

e. Provides support and testing support to the DODIN to ensure interoperability with external mission partners including other Federal Agencies and non-U.S. mission partners.

## 2.5. DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY.

Under the authority, direction, and control of the USD(I&S) and in addition to the responsibilities in Paragraph 2.8., the Director, Defense Counterintelligence and Security Agency coordinates with the USD(P&R) to:

a. Manage background investigation attributes and artifacts including status of Federal Bureau of Investigation records checks, background investigation status/final adjudication, ten-print fingerprint biometrics, and clearance attributes for individuals seeking access to DoD installations/bases and DoD information systems containing controlled unclassified and classified information.

b. Support a robust, reliable connection with the USD(P&R) for the frequent exchange of background investigation attributes and artifacts.

## 2.6. USD(P&R).

In addition to the responsibilities in Paragraph 2.8., the USD(P&R):

a. Serves as DoD's joint lead for identity management activities with the DoD CIO, pursuant to DoDIs 1000.25 and 1000.13.

b. Coordinates with the DoD CIO and the USD(I&S) on the DoD's needs for identity proofing, identity resolution, credential management, and authentication.

c. Serves as the DoD ICAM lead for person identities, including maintaining DoD's Enterprise person identity attribute repository and ICAM person identity data management/data distribution services, pursuant to DoD ICAM Strategy.

## 2.7. DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY.

Under the authority, direction, and control of the USD(P&R), and in addition to the responsibilities in Paragraph 2.8., the Director, Department of Defense Human Resources Activity, through the Director, DMDC:

a. Appoints a senior executive-level individual to serve as a deputy lead for the ICAM JPIO and to coordinate DMDC operated enterprise ICAM services. Through the ICAM JPIO lead and/or deputy leads, the Director, Department of Defense Human Resources Activity:

(1) Ensures that DoD enterprise ICAM services operated by the NSA, DISA, and DMDC meet the needs of DoD, interoperate with each other, and support interoperability with ICAM services operated by the DoD Components.

(2) Develops and maintains a DoD Enterprise ICAM Service Implementation Plan to support the DoD ICAM Strategy.

b. Establishes, operates, tests, and maintains enterprise ICAM services that support identity, credential, and authentication activities including the person data repository, defense self-service (DS) logon and a mission partner registration service.

c. Provides cybersecurity services for DMDC-operated enterprise ICAM services in accordance with DoDI 8530.01.

d. Provides subject matter expertise and technical support to DoD Components for integration with DMDC-operated enterprise ICAM services.

## 2.8. OSD AND DOD COMPONENT HEADS AND THE COMMANDANT, UNITED STATES COAST GUARD.

The OSD and DoD Component heads and the Commandant, United States Coast Guard:

a. Establish DoD Component-level governance for identity, credentialing, and authentication.

b. Establish a Component executive lead for ICAM within their respective Component.

c. Establish a DoD Component-level policy for identity, credentialing, and authentication that addresses requirements identified in this issuance.

d. Coordinate with the DoD CIO and ICAM JPIO to identify requirements for enterprise ICAM services.

e. Plan, program, and budget to support identity, credentialing, and authentication, including integrating DoD Component and COI ICAM services with DoD enterprise ICAM services as they become available.

f. Ensure all information systems owned, operated, or managed by the DoD Component meet identity, credentialing, and authentication requirements as specified in Section 3.

g. Ensure that DoD Component level, COI level, or locally implemented ICAM services that support identity, credentialing, and authentication are operated in accordance with the policy in this issuance and support interoperability and data sharing with DoD enterprise ICAM services.

h. Review and provide approval recommendations to the DoD CIO for MFA technologies, IdPs, and E2Ps requested by information systems owned, operated, or managed by the DoD Component as described in Section 4.

i. Participate in DoD ICAM review boards as required.

## 2.9. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.8., the Chairman of the Joint Chiefs of Staff:

a. Identifies, reviews, and validates identity, credentialing, and authentication requirements used by information systems that provide support for joint, allied, and coalition missions.

b. Ensures that Combatant Commanders coordinate requirements to implement this issuance with their host Military Department.

c. Coordinates implementation and integration of ICAM services that support identity, credentialing, and authentication for non-U.S. mission partners to ensure compliance with this issuance.

# SECTION 3: IMPLEMENTATION PROCEDURES

## 3.1. TERMINOLOGY.

The terms and concepts in this paragraph are critical to a consistent understanding of authentication requirements to access DoD resources:

### a. Entity.

Any person, role, organization, physical device, virtual device, or process that requests access to and uses DoD resources. Entities are provided with credentials to verify their association with a digital identity, which consists of a unique identifier that may have additional attributes bound to it.

#### (1) Person Entity.

An individual acting as themselves or in the capacity of a role that is assigned an identifier and attributes, issued credentials, and provided with entitlements to support authentication and authorization. Person entities include named individuals, organization roles (e.g., acting on behalf of an executive), and job function roles (e.g., IT privileged users).

#### (2) NPE.

A physical device, virtual machine, system, service, or process that is assigned an identifier and is issued credentials to support authentication and authorization. NPEs authenticate to information systems independent of individual actions by person entities. NPEs may be acting on behalf of a person entity, such as RPA bots, but must be independently authorized to perform any actions. Any resource that authenticates itself to person entities or other NPE resources, including web browsers is an NPE. Resources that do not authenticate themselves to person entities or other resources are not considered NPEs.

### b. DoD User Community.

DoD provides resources to a broad community of users to support its core mission. DoD information systems also provide services to beneficiaries and to address non-traditional missions such as disaster relief or community services.

#### (1) DoD Internal Community.

DoD internal community includes all entities whose identities are managed internal to DoD systems and that are issued credentials by a DoD enterprise CSP. The DoD internal community includes DoD Service members; DoD civilian employees; contractors who work on DoD computers at DoD facilities; eligible contractors who do not work at DoD facilities as defined in DoDI 1000.13; eligible non-U.S. persons who work on DoD computers at DoD facilities; roles managed by DoD; and NPEs that are managed by DoD.

(2) External Mission Partners.

DoD interacts with a broad community of mission partners who do not have credentials issued by DoD enterprise CSPs. External mission partners include Federal agency employees and provisioned contractors; DoD contractors; non-U.S. persons, including allied and coalition partners; other government representatives, including State, local, and tribal government employees, and external NPEs such as cloud service providers.

(3) Beneficiaries.

DoD provides services to individuals who are eligible for benefits because of their relationship to DoD. The DoD beneficiary community includes DoD Service members; military retirees; military spouses and other dependents; and overseas DoD civilian employees. This community may also include person entities who have been designated to represent a beneficiary, either by the beneficiary themselves or through a legal process such as dependency or power of attorney.

(4) Other Entities.

Some DoD information systems provide resources to external entities for a limited duration or purpose. These entities include vendors, third party providers such as healthcare providers, non-traditional mission non-governmental organizations, military accession applicants (recruits), and U.S. citizens.

**c. User Types.**

Requirements for authentication are dependent on the type of resources being requested.

(1) General User.

Users who require access to information resources provided by the information system but do not have additional authorities within the information system are general users.

(2) Privileged User.

Users who require access rights beyond those of a general user to perform their job function, or who require provisioned entitlements that allow them to manage the operations of information systems, network components, or resources are privileged users.

(a) Functional Privileged User.

A user who has approval authorities within workflows. Functional privileged user roles are specific to a mission area, such as human resources or finance.

(b) IT Privileged User.

A user who has roles that allow read, write, or change access to manage IT systems, including system, network, and database administrators, as well as security analysts who manage

audit logs. IT privileged user roles are generic to all IT infrastructure, including transport, DoD and commercial clouds, hosting environments, cybersecurity, and application deployment.

### d. Credentials and Authenticators.

This issuance does not use credential and authenticator interchangeably.

#### (1) Credential.

An object or data structure that authoritatively binds a digital identity, via one or more identifiers and (optionally) additional attributes, to at least one authenticator possessed and controlled by the entity associated with the digital identity. For example, a public key certificate is a credential that binds a digital identity to a public key.

#### (2) Authenticator.

Something the entity possesses and controls that is used to authenticate the entity and link it to the entity's digital identity. For example, the authenticator for PKI is the private key used by the entity to verify that the entity is associated with the digital identity in the public key certificate.

#### (3) MFA.

MFA uses more than one distinct authentication factor for successful authentication. MFA can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something the entity knows, something the entity has, and something the entity is. Non-PKI MFA credential types must be approved for use by DoD information systems through the process in Section 4.

### e. Resource Risk Levels.

NIST FIPS 199 defines low, moderate, and high impact regarding the loss of confidentiality, integrity, or availability. Requirements in this issuance relate to specific resources being requested, and focus on the assessed confidentiality risk level. For example, an information system may be assessed at an overall high confidentiality level based on the aggregate data contained within the system, but a given authentication may only provide access to a limited set of data that is assessed to be low-risk.

### f. Cryptographic Module Validation.

Cryptographic modules used by DoD must be validated through the NIST Cryptographic Module Validation Program as defined in NIST FIPS 140-3. Cryptographic modules are validated against the version of NIST FIPS 140-3 in effect when the module is tested. Cryptographic module validation certificates can be found at https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules.

(1) If a validation certificate for a cryptographic module is marked as active, the module may be procured and used for new and existing information systems.

(2) If a validation certificate for a cryptographic module is marked as historical, the module may continue to be used for the lifecycle of the system it was procured for but may not be procured for new information systems.

(3) If a validation certificate for a cryptographic module is marked as revoked, the module's validation is no longer valid and the module may not be used.

**g. Assurance Levels.**

NIST SP 800-63-3 provides an overview of general identity frameworks, using authenticators, credentials, and assertions together in a digital system, and a risk-based process of selecting assurance levels. Paragraphs 3.1.g.(1) through (3) provide summary information for the three types of assurance levels defined in NIST SP 800-63-3.

(1) Identity Assurance Level (IAL).

IAL indicates the robustness of the identity proofing process to confidently determine the identity of an individual.

(a) IAL1 permits identity and any attributes to be self-asserted.

(b) IAL2 requires identifying attributes to be verified in person or remotely as described in NIST SP 800-63A.

(c) IAL3 requires identifying attributes to be verified in person by an authorized CSP representative through examination of physical documentation as described in NIST SP 800-63A.

(2) AAL.

AAL indicates the robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier.

(a) AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol.

(b) AAL2 requires proof of possession and control of two different authentication factors through a secure authentication protocol using approved cryptographic techniques as described in NIST SP 800-63B, including cryptographic module validation as described in Paragraph 3.1.f. and medium baseline protection for verifiers.

(c) AAL3 requires proof of possession of a key through a cryptographic protocol using approved cryptographic techniques, and a hardware cryptographic authenticator that provides verifier impersonation resistance as described in NIST SP 800-63B, including verifier requirements when defining AAL levels, including cryptographic module validation as described in Paragraph 3.1.f. and high baseline protection for verifiers.

(3) Federation Assurance Level (FAL).

FAL indicates the robustness of the assertion protocol an IdP uses to communicate authentication and any additional attribute information.

(a) FAL1 permits the relying party to receive a bearer assertion from an IdP. The IdP must sign the assertion using approved cryptography.

(b) FAL2 permits the relying party to receive a bearer assertion from an IdP. The IdP must sign and encrypt the assertion using approved cryptography such that the relying party is the only party that can decrypt it.

(c) FAL3 requires the subscriber to present proof of possession of a cryptographic key reference in the assertion and the assertion artifact itself. The IdP must sign and encrypt the assertion using approved cryptography such that the relying party is the only party that can decrypt it.

**h. IdPs.**

IdPs are systems that perform direct authentication of entity authenticators and issue assertions of digital identity and optionally additional attributes based on the credentials associated with the authenticators. IdPs are used to support many different use cases. Identity Federation Service, Authentication Gateway Service, and Authentication Brokerage Service are all terms that have been previously used to describe IdPs. Requirements for IdPs are described in Paragraph 3.6.

(1) In-line reverse proxy IdPs perform authentication on behalf of one or more information systems that have physical or logical network protections that prevent remote access to the information system except through the IdP. These IdPs are used when information systems do not support required authenticators, to support reduced sign-on for users, or as part of an overall network architecture implementation. In-line reverse proxy IdPs may be referred to as "gateways" or "authentication gateways" in other documents.

(2) Break and inspect reverse proxy IdPs support terminating transport layer security (TLS) sessions at a network boundary to inspect the contents of encrypted sessions. The break and inspect process represents a reverse proxy IdP authentication where the intermediary system performing the inspection acts as the reverse proxy IdP. While these IdPs may act as general purpose IdPs and provide assertions representing the user, many break and inspect reverse proxy IdPs generate PKI certificates to represent the user. When using break and inspect proxy IdPs that generate certificates, the attributes provided to the information system are limited because not all attributes contained in the certificate used by the entity for authentication to the reverse proxy IdP are provided in the certificate issued by the reverse proxy IdP to represent the user.

(3) General purpose IdPs perform authentication and generate standards-based assertions which are provided to information systems. General purpose IdPs can either generate assertions in response to an information system request or can initiate assertions on behalf of the requesting entity and send the assertion to the information system without a prior request.

### i. Impact Levels (ILs).

Requirements for data hosted in a cloud environment are defined in the DoD Cloud Computing Security Requirements Guide (SRG) and summarized in Paragraphs 3.1.i.(1) through (4). For full definitions and descriptions, refer to the DoD Cloud Computing SRG. The DoD Cloud Computing SRG identifies four ILs: IL2, IL4, IL5, and IL6. IL1 and IL3 are no longer used. Cloud service offerings (CSO) used by DoD must be approved at the appropriate IL depending on the type of resources hosted in the cloud. Authentication performed in the cloud, either directly or through an IdP, must also take place using a CSO approved at the appropriate IL. For example, if the authentication requirements are IL4, the original authentication cannot be performed in an IL2 cloud.

#### (1) IL2.

IL2 includes all data cleared for public release as well as some low-risk unclassified information, but the information requires some minimal level of access control. IL2 CSO customers include whomever the cloud service provider chooses to market the CSO to, which may include government customers, commercial customers, and the general public. Access to the CSO is via the Internet.

#### (2) IL4.

IL4 accommodates Controlled Unclassified Information (CUI) and other mission critical data including that used in direct support of military or contingency operations. IL4 CSOs may support a U.S. Government community or a DoD-only community. Commercial IL4 CSO customers include all U.S. Government customers (i.e., Federal, State, local, and tribal) and commercial customers that support them. In some cases, an IL4 CSO may support other commercial entities, but not the general public.

#### (3) IL5.

IL5 accommodates CUI that may require a higher level of protection than that afforded by IL4, as deemed necessary by the information owner, public law, or other government regulation. IL5 also supports unclassified national security infrastructure. IL5 CSOs may support a Federal Government community or a DoD-only community. Commercial IL5 CSO customers include all Federal Government customers (Federal agencies only) which includes DoD Components and certain DoD contractors operating a DoD system on behalf of DoD.

#### (4) IL6.

IL6 accommodates information that has been classified up to Secret. IL6 CSOs may support a Federal Government community or a DoD-only community. IL6 CSOs may only be provided by cloud service providers under contract to DoD or another Federal department or agency.

## 3.2. GENERAL AUTHENTICATION.

This paragraph discusses general authentication requirements that are applicable to person entities and NPEs.

a. Person entities must be authenticated in accordance with Paragraph 3.3. NPEs must be authenticated in accordance with Paragraph 3.4.

b. Credentials and authenticators used for authentication must either be issued by a DoD enterprise ICAM service, issued by an external PKI approved in accordance with DoDI 8520.02, or must meet the identity proofing and credential requirements described in Paragraph 3.5.

(1) MFA technologies must be approved in accordance with Paragraph 4.1.

(2) Memorized secrets and lookup secrets including passwords must meet the requirements in Paragraph 3.5.a.(3).

(3) Other cryptographic device and cryptographic software authenticators such as Secure Shell (SSH) keys must meet the requirements in Paragraph 3.5.a.(4).

c. Information systems may rely on assertions provided by an IdP in lieu of direct authentication if the IdP is operated in accordance with Paragraph 3.6. and is either a reverse proxy IdP or has been approved in accordance with Paragraph 4.2.

d. This issuance replaces sensitivity levels, credential strengths, and entity environments previously defined, and updates previously defined use cases.

(1) Sensitivity levels have been replaced with low-, moderate-, and high-risk. Sensitivity levels 1 and 2 generally align with low-risk resources. Sensitivity levels 3, 5, and 6 generally align with moderate-risk resources. Sensitivity levels 4 and 7 generally align with high-risk resources.

(2) Credential strengths have been replaced by specific references to credential types throughout the issuance. Credential strength A and F generally align with username and password and other single-factor credentials that are AAL1. Credential strength B generally aligns with MFA credentials that are AAL2. Credential strengths C and G generally align with software public key certificates which are also AAL2. Credential strengths D, E, and H generally align with hardware public key certificates that are AAL3. When required, a U.S. Government adjudicated background investigation must be completed either as part of the credential issuance process or be independently verified before granting access.

(3) Entity environments have been incorporated into compensating controls and are defined within each of the authentication requirements for each risk level.

(4) Information systems with a previously approved use case or E2P must evaluate their implementation and request a new E2P if their use case is not addressed in this issuance.

(5) MFA technologies and IdPs (also known as identity federation services) retain their approval status until specifically rescinded. A full list of approved MFA technologies and IdPs can be found at https://intelshare.intelink.gov/sites/dodcioicamdocs.

## 3.3. PERSON ENTITY AUTHENTICATION REQUIREMENTS.

All person entities requesting access to DoD resources must be authenticated, unless the resource has been approved for public release in accordance with DoDIs 5230.09 and 5230.29, or the information system is intended for public collaboration where unauthenticated guest access is approved. Most information systems authenticate different types of users as outlined in Paragraph 3.1.c. Each authentication event from a person entity must meet the minimum requirements for the risk level of the resources being requested. Authenticated users seeking elevation of privileges (e.g., from a general user to a functional privileged user) must be re-authenticated if the initial authentication did not meet the requirements for the additional resources or actions being requested, or for an IT privileged user, using the credential used for IT privileged user functions. This paragraph defines requirements for authenticating person entities based on the risk of loss of confidentiality, integrity, and availability of the resource to DoD. These requirements apply for unclassified and classified resources. For classified resources, these requirements are in addition to existing network and data encryption requirements.

### a. Authentication for Access to Low-Risk Resources.

Authentication for access to low-risk resources must be performed as specified in either Paragraph 3.3.a.(1) or Paragraph 3.3.a.(2). If the IdP or information system performing the initial authentication is cloud-based, the authentication action must be performed within an IL2 or higher CSO for unclassified resources, or IL6 for Secret resources.

#### (1) Authentication Requirements without Compensating Controls.

The approaches described in Paragraphs 3.3.a.(1)(a) through (c) are approved for authentication to access low-risk resources.

##### (a) Direct.

Information systems may use DoD-approved MFA for direct authentication. Information systems must also support the use of public key certificates issued by a DoD-approved PKI for direct authentication.

##### (b) Assertion Based.

Information systems may use assertions provided by an approved IdP for authentication provided the IdP authenticated the entity using a DoD-approved AAL2 authenticator. Assertions generated by in-line IdPs may use any format supported by the information system provided that the information system cannot be accessed except through the in-line IdP. Assertions generated by general purpose IdPs must:

1. Indicate that the original authentication met AAL2 and IAL2 requirements.

2. Meet FAL1 requirements.

(c) DS Logon Assertion Based.

Information systems may use assertions provided by DS logon for authentication provided the assertion meets FAL1.

(2) Authentication Requirements with Compensating Controls.

Authentication using single-factor AAL1 authenticators as defined in NIST SP 800-63B may be used where at least one of the compensating controls listed in Paragraphs 3.3.a.(2)(a)-(g) is in place. Authenticators must be managed in accordance with the requirements in Paragraph 3.5.

(a) Physical Access Controls.

Standalone systems and information systems that are part of closed restricted networks that are not externally connected to live operational networks; do not have the ability to access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that have commensurate physical controls that restrict access to only authorized users.

(b) Temporary Access.

Information systems that provide access for a limited period of time to support a specific action, such as employment application, proposal submission, conference registration, or activities related to a permanent change of station moves.

(c) Schoolhouse or Other Training Environments.

Information systems that only host resources used to support students in schoolhouse environments or are only used to provide training that do not contain DoD CUI other than the individual's own personally identifiable information (PII).

(d) Development, Labs, Ranges, or Test Environments.

Information systems that collect or process test data that are either not externally connected to live operational networks or that have highly constrained connections that only permit one-way transfer of test data to the operational network and do not permit authentication from the operational network.

(e) Development Support Systems.

Information systems that primarily support system development where the authenticator is stored on an endpoint that is actively managed by a DoD Component or DoD mission partner and meets DoD standards for endpoint hardening on a DoD managed device.

(f) Medical Devices.

Special purpose information systems that are used for diagnostic or interventional care that do not support MFA authentication when used in accordance with their medical compliance requirements.

(g) Nontraditional Mission Partner Systems.

Information systems that are specifically intended to rapidly engage DoD mission partners in nontraditional missions such as humanitarian assistance, disaster response, or stability operations.

(3) Use Cases.

Low risk use cases often support activities that are outside of the core DoD mission, provide access to very limited information, or are restricted to accessing information specific to the entity being authenticated. Low risk access includes, but is not limited to:

(a) Inputting, reviewing, or modifying self-asserted personal information such as a credit card number, job application, or contact information by the person or their designee.

(b) Reviewing own training records by a person or their designee.

(c) Pre-accession recruits, reservists, and National Guard members who have not yet been registered in the person data repository and have not been issued a CAC, accessing resources related to their own record.

(d) Inputting, reviewing, or modifying company proprietary information such as proposals, contracts, or trade secrets by a representative linked to that company.

(e) Inputting, reviewing, or modifying PII, protected health information, or other beneficiary information by the beneficiary or their designee.

(f) Interactions with suppliers and other vendors related to specific transactions with that supplier or vendor.

(g) Managing configuration of medical devices or collecting information generated by medical devices.

(h) Accessing information resources to support nontraditional missions such as humanitarian assistance, disaster response, or stability operations.

(i) Accessing information systems that provide resources to support students in schoolhouse environments or are only used to provide training.

(j) Accessing test or training data randomly generated or otherwise not related to real world data in development and test systems even if a production system will host moderate or high risk resources. All development, lab, range, and test accounts must be disabled or

transitioned to requiring production-level credentials for authentication before migrating the information system into production status.

(k) Accessing information systems that provide resources that only support morale, welfare, and recreation activities.

(l) Accessing development support systems.

**b. Authentication for Access to Moderate Risk Resources.**

Authentication for access to moderate-risk resources must be performed as specified in either Paragraph 3.3.b.(1) or (2). If the IdP or information system performing the initial authentication is cloud-based, the authentication action must be performed within an IL4 or higher CSO for unclassified resources, or IL6 for Secret resources, respectively.

(1) Authentication Requirements without Compensating Controls.

The approaches described in Paragraphs 3.3.b.(1)(a) and (b) are approved for authentication to access moderate-risk resources.

(a) Direct.

Information systems may use hardware public key certificates from a DoD-approved PKI for direct authentication.

(b) Assertion Based.

Information systems may use assertions provided by an approved IdP for authentication provided the IdP authenticated the entity using a DoD-approved AAL3 credential. Assertions generated by in-line IdPs may use any format supported by the information system provided that the information system cannot be accessed except through the in-line IdP. Assertions generated by general purpose IdPs must:

1. Indicate that the original authentication met AAL3 and IAL2 requirements.

2. Meet FAL1 requirements if the assertion was generated in response to an information system request.

3. Meet FAL2 requirements if the assertion was initiated by the requesting entity.

(2) Authentication Requirements with Compensating Controls.

The authentication mechanisms described in Paragraphs 3.3.b.(2)(a) through (e) may be used when the appropriate compensating controls described in the paragraphs are in place.

(a) Physical Access Controls.

Standalone systems and information systems that are part of closed restricted networks that are not externally connected to live operational networks; do not have the ability to

access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that have commensurate physical controls that restrict access to only authorized users, may use single factor authenticators such as username and password or approved MFA for authentication.

(b) Managed Endpoint.

Information systems may use software public key certificates from a DoD-approved PKI for authentication if the information system is able to verify that the endpoint the entity is being used to authenticate from is actively managed by a DoD Component or DoD mission partner and meets DoD standards for endpoint hardening. DoD managed mobile phones and DoD managed NPEs are examples of managed endpoints.

(c) Federated Mission Partner Environments.

Information systems that provide access to resources based on country of origin may accept assertions from an approved IdP for that country that meets AAL3 requirements even if the IdP authenticated the entity using an AAL2 credential that is approved for use by the country of origin.

(d) Operationally Constrained Environment.

1. Information systems in operationally constrained environments, such as denied, degraded, intermittent, or limited bandwidth (DDIL) environments, where PKI based authentication is constrained by the available network infrastructure or other environmental considerations, may use software public key certificates from a DoD-approved PKI or use a DoD-approved MFA for authentication leveraging cached revocation information, provided that the revocation status information is updated when bandwidth is available.

2. If the system cannot support public key certificate or MFA based authentication, the system may use single factor authenticators such as username and password if commensurate controls are also enforced for access to those authenticators. The authorizing official (AO) for the information system must approve the authentication mechanism based on an assessment of the risks, capabilities, and operational environment.

(e) Crisis Situation.

Information systems may use software public key certificates from a DoD-approved PKI, DoD-approved MFA, or username and password for authentication for emergency accounts that are established in response to crisis situations. These accounts must be disabled when normal operations resume. These accounts must also be set to automatically disable after a preset amount of time based on the anticipated duration of the situation.

(3) Use Cases.

Most resources that support the core DoD mission are moderate-risk. Moderate-risk access includes, but is not limited to:

(a) Logging onto provisioned DoD network accounts.

(b) Accessing CUI (regulatory sensitive information for which access is limited by law, regulation, or other mandate) except as described in Paragraphs 3.3.a. and 3.3.c.

(c) Accessing payroll, finance, logistics, and personnel management information as a functional privileged user that can view PII or protected health information for multiple people as part of their job function (functional privileged users do not include designees that are supporting multiple beneficiaries).

(d) Accessing closed coalition mission networks supporting operations.

(e) Accessing information systems containing low and moderate-risk resources as a functional privileged user.

### c. Authentication for Access to High-Risk Resources.

Authentication for access to high risk resources must be performed as specified in either Paragraph 3.3.c.(1) or (2). If the IdP or information system performing the initial authentication is cloud-based, the authentication action must be performed within an IL5 or higher CSO for unclassified resources, or IL6 for Secret resources.

#### (1) Authentication Requirements without Compensating Controls.

The approaches described in Paragraphs 3.3.c.(1)(a) and (b) are approved for authentication to access high-risk resources.

##### (a) Direct.

Information systems may use hardware public key certificates from a DoD-approved PKI for authentication.

##### (b) Assertion Based.

Information systems may use assertions provided by an approved IdP for authentication, provided the IdP authenticated the entity using a DoD-approved AAL3 authenticator. Assertions generated by in-line IdPs may use any format supported by the information system provided that the information system cannot be accessed except through the in-line IdP. Assertions generated by general purpose IdPs must:

1. Indicate that the original authentication met AAL3 and IAL2 requirements.

2. Meet FAL2 requirements if the assertion was generated in response to an information system request.

3. Meet FAL3 requirements, if the assertion was initiated by the requesting entity.

(2) Authentication Requirements with Compensating Controls.

The authentication mechanisms described in Paragraphs 3.3.c.(2)(a) through (g) may be used when the following appropriate compensating controls are in place:

(a) Physical Access Controls.

Standalone systems and information systems that are part of closed restricted networks that are not externally connected to live operational networks that do not have the ability to access the network infrastructure, cannot transmit, receive, route, or exchange information outside of the system or network boundary, and that reside in physical spaces that have commensurate physical controls that restrict access to only authorized users may use single-factor authenticators such as username and password or approved MFA for authentication.

(b) Operationally Constrained Environment.

1. Information systems in operationally constrained environments, such as DDIL environments, where PKI based authentication is constrained by the available network infrastructure or other environmental considerations, may use software public key certificates from a DoD-approved PKI or use a DoD-approved MFA for authentication.

2. If the system cannot support public key certificate or MFA-based authentication, the system may use single-factor authenticators such as username and password if commensurate controls are also enforced for access to those authenticators. The AO for the information system must approve the authentication mechanism based on an assessment of the risks, capabilities, and operational environment.

(c) Crisis Situation.

Information systems may use software public key certificates from a DoD-approved PKI, DoD-approved MFA, or username and password for authentication for emergency accounts that are established in response to crisis situations. These accounts must be disabled when normal operations resume and set to automatically disable after a preset amount of time based on the anticipated duration of the situation.

(d) IT Privileged User Account.

When information systems do not support PKI or MFA authentication for IT privileged accounts, these accounts must either be disabled from remote access or must use a third-party administration tool that requires hardware public key certificate logon for access to the authenticator for the account, and must change these account authenticators at least weekly. If fully automated authenticator changes are supported, authenticators must be changed within one hour of each account usage.

(e) IT Device Local Logon.

Information systems may use username and password for local logon accounts for IT privileged users that are used when network access or normal logon is unavailable. These

accounts must not be used at any other time, must be restricted from remote access, and systems must reside in physical spaces that restrict access to only authorized users.

(f) Endpoint Local Logon.

Endpoint systems may use username and password for local logon accounts for IT privileged users. These accounts must be restricted from remote access, and systems must either reside in physical spaces that restrict access to only authorized users or must have a capability to remotely lock or zeroize the device if the device is no longer under the positive control of the intended user.

(g) IT Privileged Access to Manage CSO.

1. When management interfaces for CSOs do not support PKI authentication for IT privileged accounts, these accounts must use DoD-approved MFA authenticators. As a compensating control, access to at least one of the factors must require authentication using a DoD-approved PKI authenticator so that DoD PKI revocation procedures will apply to the alternative implementation.

2. The information system AO may temporarily accept the risk of using an MFA technology that has not yet been approved in accordance with Paragraph 4.1. based on an assessment of the risks, capabilities, and operational environment, provided that the authenticator technology has been submitted for approval.

(3) Use Cases.

Some resources that support the core DoD mission, including operationally sensitive information are high risk. High-risk access includes, but is not limited to

(a) Accessing CUI from unclassified networks where unauthorized access to or compromise of the CUI could result in severe mission capability degradation, major damage to a DoD information based resource, or a risk of serious injury or death to personnel but that has not been specifically authorized to be classified. Types of CUI include combat mission, law enforcement, or unclassified controlled nuclear information.

(b) Accessing information systems as an IT privileged user.

(c) Authentication to CSO management of application programming interface.

## 3.4. NPE AUTHENTICATION REQUIREMENTS.

NPEs requesting access to DoD resources or exchanging information with DoD resources must be authenticated, unless the resource has been approved for public release in accordance with DoDIs 5230.09 and 5230.29. This paragraph defines requirements for authenticating NPEs based on the type of transaction. These requirements apply for both unclassified and classified resources. For classified resources, these requirements are in addition to existing network and data encryption requirements.

### a. NPE Authentication to Support Mutually Authenticated Transactions.

To support mutually authenticated transactions, the NPE information system hosting DoD resources must be able to authenticate itself to the entity requesting access to a DoD resource or to a third-party controller managing the connection.

#### (1) Authentication Requirements without Compensating Controls.

NPE information systems must use software or hardware public key certificates from a DoD-approved PKI for authentication in accordance with DoDI 8520.02.

#### (2) Authentication Requirements with Compensating Controls.

##### (a) Physical Access Controls.

Authentication using single-factor authenticators may be used by NPE information systems that are part of closed restricted networks that are not externally connected to live operational networks; do not have the ability to access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that restrict access to only authorized users.

##### (b) Operationally Constrained Environment.

1. Information systems in operationally constrained environments, such as DDIL environments, where PKI-based authentication is constrained by the available network infrastructure or other environmental considerations, may use DoD-approved MFA for authentication.

2. If the system cannot support public key certificate or MFA-based authentication, the system may use single-factor authenticators such as username and password if commensurate controls are also enforced for access to those authenticators. The AO for the information system must approve the authentication mechanism based on an assessment of the risks, capabilities, and operational environment.

#### (3) Use Cases.

Mutual authenticated transaction includes, but is not limited to:

(a) DoD web server authenticating itself to a web browser as part of establishing a TLS session. DoD web servers must use public key certificates issued by a PKI that is trusted by the intended web browser clients as defined in DoDI 8520.02.

(b) DoD service authenticating itself before establishing a TLS session. DoD services must use public key certificates issued by a PKI provider that is trusted by the intended client as defined in DoDI 8520.02.

(c) System authenticating itself as part of initiating a session in a zero trust environment.

### b. NPE Device Authentication to Network.

Access to DoD operated networks requires the endpoint device to be authenticated before allowing user authentication.

#### (1) Authentication Requirements without Compensating Controls.

NPE endpoint or mobile devices must use software or hardware public key certificates from a DoD-approved PKI for authentication in accordance with DoDI 8520.02.

#### (2) Authentication Requirements with Compensating Controls.

The authentication mechanisms described in Paragraphs 3.4.b.(2)(a) and (b) may be used when appropriate compensating controls are in place.

##### (a) Physical Access Controls.

Authentication using single-factor authenticators may be used by NPE devices that are part of closed restricted networks that are not externally connected to live operational networks; do not have the ability to access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that restrict access to only authorized users. Memorized secrets and lookup secrets must be managed in accordance with the requirements in Paragraph 3.5.

##### (b) Operationally Constrained Environment.

1. Information systems in operationally constrained environments, such as DDIL environments, where PKI-based authentication is constrained by the available network infrastructure or other environmental considerations, may use DoD-approved MFA for authentication.

2. If the system cannot support public key certificate or MFA-based authentication, the system may use single factor authenticators such as username and password if commensurate controls are also enforced, for access to those authenticators. The AO for the information system must approve the authentication mechanism based on an assessment of the risks, capabilities, and operational environment.

##### (c) Guest Networks.

Networks that do not provide access to any DoD resources except those approved for public release, such as Wi-Fi networks that only provide internet connectivity, do not need to authenticate NPE devices accessing the network.

#### (3) Use Cases.

Device authentication includes, but is not limited to:

(a) Endpoint device authenticating to a network domain controller.

(b) Endpoint device remotely authenticating to a network as part of establishing a virtual private network connection.

(c) Endpoint device authenticating itself as part of initiating a session in a zero trust environment.

### c. NPE Authentication to Static NPE.

Information system NPEs may authenticate to each other based on static connection agreements. These agreements may be included in the definition of the information system's boundary, and may incorporate a memorandum of agreement established between organizations whose systems are interconnected.

#### (1) Authentication Requirements without Compensating Controls.

NPEs must use software or hardware public key certificates from a DoD-approved PKI for authentication in accordance with DoDI 8520.02.

#### (2) Authentication Requirements with Compensating Controls.

Authentication using single-factor authenticators may be used where at least one of these compensating controls are in place. Authenticators must be changed if information system NPEs are transitioned from development or test status to operational use cases.

##### (a) Physical Access Controls.

Standalone systems and information system NPEs that are part of closed restricted networks that are not externally connected to live operational networks; do not have the ability to access the network infrastructure; cannot transmit, receive, route, or exchange information outside of the system or network boundary; and that reside in physical spaces that restrict access to only authorized users.

##### (b) Operationally Constrained Environment.

1. Information systems in operationally constrained environments, such as DDIL environments, where PKI-based authentication is constrained by the available network infrastructure or other environmental considerations, may use DoD-approved MFA for authentication.

2. If the system cannot support public key certificate or MFA-based authentication, the system may use single factor authenticators such as username and password if commensurate controls are also enforced for access to those authenticators. The AO for the information system must approve the authentication mechanism based on an assessment of the risks, capabilities, and operational environment.

##### (c) Dedicated Connectivity.

Systems that have a physical or virtual dedicated connection to each other such that no other system can access the connection and impersonate the system.

(3) Use Cases

Static system authentication includes, but is not limited to:

(a) Establishing a router mesh network or router-to-router communication.

(b) Two or more servers with defined high-throughput connections to exchange information.

(c) Dedicated imagery circuits and uplinks at Combatant Commands.

**d. NPE Authentication to Support CSO Management**

Information system NPEs may authenticate to each other based on static connection agreements. These agreements may be included in the definition of the information system's boundary, and may incorporate a memorandum of agreement established between organizations whose systems are interconnected.

(1) Authentication Requirements without Compensating Controls.

NPEs must use software or hardware public key certificates from a DoD-approved PKI for authentication in accordance with DoDI 8520.02.

(2) Authentication Requirements with Compensating Controls.

When management interfaces for CSOs do not support PKI authentication, the system may use single-factor AAL1 authenticators. Use of these authenticators must be documented in the security plan provided by the vendor and approved by the DoD Cloud Authorization Service.

(3) Use Cases

Static system authentication includes, but is not limited to:

(a) Authentication of tools to a cloud API.

(b) Establishment of the integration between a CSO and an IdP.

**e. NPE Authentication as a Provisioned User.**

NPEs may be processes acting as authorized entities that authenticate to information systems.

(1) Authentication Requirements.

Authentication requirements for these NPEs, including baseline and compensating controls, are the same as the requirements in Paragraph 3.3., depending on the risk classification of the resource being accessed.

(2) Use Cases.

NPE authentication to services includes, but is not limited to:

(a) Web services, application programming interfaces, and other software entities acting autonomously.

(b) Backup or other processes initiated by an external information system.

(c) Unattended RPA bot.

(d) Monitoring tools that require access to the monitored system including automated network scans, vulnerability scans, and host based security systems.

(e) Scripts, automation, and orchestration processes that perform network management or other tasks.

## 3.5. CSP REQUIREMENTS.

A CSP issues authenticators and associated credentials to subscribers, including person entities and NPEs. CSPs are responsible for managing the digital identities associated with credentials, as well as the credentials themselves, including issuance, maintenance, revocation, and any privacy impact assessments or System of Records Notices required by the collection, storage, and use of PII. Information systems that authenticate users based on credentials issued by a DoD enterprise CSP or DoD-approved CSP can rely on DoD enterprise or DoD-approved CSP for identity management and credential management.

### a. Credential and Authenticator Technology.

CSPs must meet the requirements described in Paragraphs 3.5.a.(1) through (3), depending on the type of credential being issued. Authenticators used to authenticate resources hosting resources are considered classified at the same level as the resource being accessed and must be protected accordingly.

#### (1) PKI.

Requirements for public key certificates and DoD approval of PKIs are described in DoDI 8520.02.

#### (2) MFA.

CSPs supporting MFA, including those that use cryptographic tokens and one-time passwords as one of the authenticators, must:

(a) Meet all requirements for AAL2 defined in NIST SP 800-63B.

(b) Use MFA technologies that have been approved for use by DoD information systems using the process described in Paragraph 4.1.

(c) Meet the requirements listed in Paragraph 3.5.a.(3) when one of the factors is a username and password.

(3) Memorized Secrets and Lookup Secrets.

CSPs supporting username and password based authentication in accordance with Paragraphs 3.3. and 3.4. must implement requirements in Paragraphs 3.5.a.(3)(a) through (d). Systems that cannot support these requirements must implement compensating controls that limit network access to the system, such as requiring physical presence for password entry or installing an in-line IdP between the network and the information system.

(a) Meet all requirements for memorized secrets as defined in NIST SP 800-63B.

(b) Require passwords to be at least fourteen characters long. Passwords must support all printable American standard code for information interchange characters.

(c) Store passwords in a form that is resistant to offline attacks. Salt and hash secrets using a suitable one-way key derivation function that takes the secret, a salt, and a cost factor as inputs then generates a hashed secret. The salt must be at least 32 bits in length and be generated by a NIST FIPS 140-3 compliant random number generator to mitigate the use of rainbow tables by threat actors. Store both the salt value and the resulting hash for each user using a memorized secret authenticator.

(d) Mitigate online attacks where the attacker attempts to log in by guessing the password by limiting the rate of login attempts permitted and implementing account lockout after a maximum number of failed logon attempts has been reached. The maximum number must be approved by the information system's AO based on the operational needs of the system.

(4) Single Factor Cryptographic Authenticator.

Single factor cryptographic authenticators such as SSH must meet the requirements of NIST SP 800-131A. Services leveraging single factor cryptographic keys must provide secure communication channels (e.g. TLS, SSH) for client connectivity. Clients must only submit its client authenticator using the service's secure communication channel after verifying the service's authenticator.

**b. Identity Proofing.**

CSPs must verify the identity of the entity prior to issuing a credential to that entity using one of the methods in Paragraphs 3.5.b.(1) through (4). The method for identity proofing must be documented by the CSP and must be reviewed and approved by the AO for the CSP.

(1) Self-Asserted.

Self-asserted identity may only be used for low-risk access where information resources provided to the entity are not CUI and where PII is limited to that provided by the entity as part of the registration process. Examples of where self-asserted identity may be used include information systems supporting civilian job application or military recruiting, conference registration, and registration to receive requests for proposals or submit proposals. Acceptance of a public key certificate issued by a PKI provider that is not DoD-approved in order to establish a TLS session with an external web site is also considered a self-asserted identity. Self-asserted identity proofing meets IAL1.

(2) Authentication with a DoD-approved Credential.

Identity proofing may be performed through electronic validation of an existing DoD-approved credential. The IAL of the new credential is the same as the IAL of the credential used. Examples of authentication using a DoD-approved credential include registration for public key certificates to support mobile devices using a CAC and validation of a CAC on NIPRNET workstation prior to issuing an MFA credential for a closed restricted network.

(a) Where authentication of an existing DoD-approved credential is used, the CSP must maintain a record of the identifier from the existing credential linked to the digital identity record for the new credential. The CSP may include the identifier in the new credential.

(b) Unless there are form factor technology or network connectivity constraints, information systems must be configured to use existing DoD-approved credentials without requiring entities to obtain a new credential.

(3) Documentation Based.

(a) Identity proofing for person entities may be performed through either in-person visual verification or approved supervised remote visual verification of existing identity documents, such as a passport, driver's license, or other government-issued identity credential. At least one of the documents used for identity proofing must contain a photograph of the person entity.

(b) In addition, the individual reviewing the documents must be familiar enough with the type of documents being presented to verify key anti-tamper features of the documents. Identity proofing based on presentation of documentation meets IAL2 or IAL3 if all of the requirements for documentation presentation and data collection defined in NIST SP 800-63A are met.

(4) Third-Party Vouching.

Identity proofing may be performed by a third-party vouching for the identity of the entity. Examples of third-party vouching identity proofing for person entities are registration of first responders and registration of coalition partner representatives. Identity proofing based on third-party vouching is not assigned an IAL in NIST SP 800-63A, as it is dependent on the identity proofing of the third party and the relationship between the third party and the entity.

(a) The third-party must be able to provide proof of its own identity using one of the methods described in Paragraph 3.5.b.(2) or 3.5.b.(3)

(b) The third-party must be a known representative of an organization that the CSP has an existing relationship with.

(c) Third-party vouching identity proofing may only be performed for access to low risk resources or where credential or documentation-based identity proofing is not possible.

(5) NPE Identity Proofing.

(a) Initial identity proofing for NPEs is generally performed by the sponsor of the NPE acting as the third-party vouching for the identity of the NPE. Some NPEs support authentication with their existing credential to request a new credential, while others require third-party vouching for each credential issued.

(b) Where NPEs support cryptographic attestations as a root of trust, these attestations should be leveraged to prove key provenance and genuineness from a supply chain perspective. Identity proofing of NPEs is not addressed in NIST SP 800-63A.

**c. Credential Issuance.**

(1) CSPs must establish a digital identity and generate credentials that contain identifiers that are unique across the set of information systems that will use the credential. Identifiers must not be reused except when issuing a new credential to the entity assigned to the identifier.

(2) CSPs must provide associated authenticators to the entity using a process that prevents anyone other than the entity from having access to the authenticator. Where third-party vouching is used for identity proofing, the authenticator may be provided to the third party to provide it to the entity.

**d. Credential Maintenance.**

CSPs must maintain credentials, including:

(1) Providing a mechanism for resetting or reissuing authenticators that are lost or forgotten that enforce identity proofing requirements.

(2) Disabling credentials that have not been used for a specified period of time.

(3) Revoking or otherwise disabling credentials when either the entity is no longer authorized to hold the credential or the credential is compromised.

## 3.6. IDP REQUIREMENTS.

Information systems may only rely on assertions provided by an IdP in lieu of direct authentication if the IdP is operated in accordance with this paragraph.

**a. In-Line Reverse Proxy IdP.**

In-line reverse proxy IdPs must:

(1) Have an authorization to operate (ATO) at a risk level commensurate with the risk level of resources hosted by information systems they support. Specifically, if the IdP will provide assertions to support authentication to resources defined as moderate- or high-risk as described in Paragraph 3.3., the ATO for the IdP must also be at moderate or high respectively.

(2) Provide customized authentication assertions to each information system they support using a format that can be consumed by the information system.

**b. Break and Inspect Reverse Proxy IdP.**

Break and inspect reverse proxy IdPs may act as general purpose IdPs and provide assertions representing the user, or may generate PKI certificates to represent the user.

(1) Break and inspect reverse proxy IdPs that generate assertions must meet the requirements identified in Paragraph 3.6.c.

(2) Break and inspect reverse proxy IdPs that generate certificates to represent the user must meet the requirements in Paragraphs 3.6.b.(2)(a) through (f) and:

(a) Be operated in accordance with the U.S. DoD Web Content Filter X.509 Certificate Policy.

(b) Maintain a Certification Practice Statement that documents technical, process, and security controls for the issuance of PKI certificates.

(c) When available, use a certification authority product that has been validated in accordance with the NIAP Protection Profile Module for SSL/TLS Inspection Proxy. If no validated products are available, then approval from the Director, NSA is required for national security systems.

(d) Have an ATO at a risk level commensurate with the risk level of information systems accepting assertions from the IdP.

(e) Limit trust in certificates issued by the IdP to only those information systems specifically intended to integrate with the IdP.

(f) Be audited at least annually to verify operation is in accordance with its Certification Practice Statement and the U.S. DoD Web Content Filter X.509 Certificate Policy. The auditor must demonstrate competence in the field of compliance audits and must be sufficiently organizationally separated from the audited party to provide an unbiased, independent evaluation.

**c. General Purpose IdP.**

General purpose IdPs may be operated by DoD or by external mission partners.

(1) DoD enterprise-, Component-, and COI-operated IdPs must have an ATO at a risk level commensurate with the risk level of resources managed by information systems accepting assertions from the IdP, and must meet all of the requirements described in Paragraphs 3.6.c.(4)(a) through (m).

(2) General purpose IdPs must be approved for use by DoD information systems as described in Section 4.

(3) General purpose IdPs used to support access to cloud-based resources must be approved for use on the IL where the resource resides.

(4) General purpose IdPs will meet the requirements in Paragraphs 3.6.c.(4)(a) through (m), which will be used when reviewing IdPs for approval.

(a) Provide assertions that contain a persistent identifier for the authenticated entity.

(b) Support assertion standards used by information systems it supports, such as security assertion markup language, OpenID Connect, and web authentication.

(c) Maintain documentation that describes technical, process, and security controls for the operation of the IdP.

(d) Be audited at least annually to verify that operation is in accordance with the IdP's documentation. The auditor must demonstrate competence in the field of compliance audits and must be sufficiently organizationally separated from the audited party to provide an unbiased, independent evaluation.

(e) Either use a signing public key certificate issued by a DoD-approved PKI or use an out-of-band process with each information system that will rely on assertions from the IdP in order to verify the public key associated with the signing private key.

(f) Require two-party control for operations involving configuration of the private key used to sign assertions.

(g) Digitally sign all assertions in accordance with FAL1.

(h) Support encryption of assertions if access to resources that will be facilitated by the IdP requires FAL2 or FAL3 as described in Paragraph 3.3.

(i) Support subscriber proof of possession of a cryptographic key reference in assertions if access to resources that will be facilitated by the IdP requires FAL3 as described in Paragraph 3.3.

(j) Include information on the authenticator type of the original authentication in assertions or be restricted for use at the lowest AAL supported by the IdP.

(k) Protect its own signing keys using a validated cryptographic module as described in Paragraph 3.1.f. IdPs that provide AAL3 assertions must protect signing keys using a Level 2 hardware or higher validated cryptographic module.

(l) Actively monitor for adversarial activity and provide immediate alerts for critical events to a certified and accredited cyber security service provider.

(m) Log all authentication requests and maintain logs sufficient to support review of logs for evidence of fraudulent activity.

# SECTION 4: APPROVAL PROCESSES

## 4.1. MFA TECHNOLOGY.

MFA technologies, including specific implementation methods, must be approved for use by DoD information systems in accordance with the process described in Paragraphs 4.1.a. through g. MFA technologies may be vendor products or may be implementations of open source specifications. Information system owners may evaluate MFA technologies in laboratory, test, and development environments to determine if they are suitable for operational use before submitting the technology for approval. MFA technologies may not be implemented in production environments until approval has been obtained. A full list of approved MFA technologies is available at https://intelshare.intelink.gov/sites/dodcioicamdocs (permission required).

a. Information system owners should leverage previously approved MFA technologies when possible. Use of previously approved MFA technologies and implementation methods does not require an additional approval provided that use of the MFA follows the approved implementation of the MFA solution. Requests for approval of new MFA technologies when previously approved MFA technologies will not meet requirements must be sponsored by an information system owner or a DoD Component. Approvals may be reevaluated based on changes to vendor capabilities or changes in DoD risk profiles.

b. Information system owners will be responsible for developing and implementing processes for credential management and identity proofing, as described in Paragraph 3.5., when deploying approved MFA technology credentials.

(1) The sponsor will compile:

(a) A description of the technology and processes for the MFA technology, including the technology used by the solution, the vendor or vendors providing the solution if applicable, whether any vendors are partially or wholly foreign-owned, and whether implementation of the solution will be hosted within DoD or requires a reach-back to vendor systems in a public or hybrid cloud. Information system owners should contact their DoD Component Supply Chain Risk Management Office to verify ownership and any other known issues regarding the vendor.

(b) Information regarding the validation status of the cryptographic modules used to support the MFA technology as described in Paragraph 3.1.f.

(c) An explanation of how the MFA technology addresses a DoD need.

(e) Description of how the MFA technology meets AAL2 or AAL3 requirements and whether the MFA technology has been independently verified by a third party as meeting the claimed AAL.

(f) Results from testing or analysis regarding the security and efficacy of the solution, including any certifications such as cryptographic module validation or NIAP protection profile validation. MFA technologies that will be used to support authentication to

national security systems must demonstrate compliance with the requirements of the NIAP program or be NSA approved in accordance with the Committee on National Security Systems Policy No. 11.

(2) The sponsor will obtain a memo recommending approval from the information system AO or the Component CISO that includes acceptance of risk for using the MFA technology.

c. The sponsor will submit the required information and recommendation for approval to the DoD CIO ICAM lead.

d. The DoD CIO ICAM lead will coordinate a review of the request with the appropriate governance body as defined by the DoD CIO or delegated Deputy DoD CIO, and, if recommended for approval, develop a draft approval memorandum that contains applicable guidance including specific implementation methods and whether the MFA technology is approved for use by the national security system.

e. If existing security review documentation is not sufficient, the DoD CIO ICAM lead may also request a security review of the MFA technology from the NSA.

f. The DoD CIO will review the request and approve or disapprove it. If approved, the DoD CIO or delegated Deputy DoD CIO will sign the approval memorandum. If disapproved, the DoD CIO ICAM lead will provide the sponsor with the reason the request was disapproved.

g. If the request is approved by the DoD CIO, the DoD CIO ICAM lead will provide the approval memorandum to the requestor, and add the approval to the appropriate published list of MFA technology.

h. The DoD CIO ICAM lead coordinates with DISA, as appropriate, to develop implementation guidance.

## 4.2. GENERAL PURPOSE IDP.

General purpose IdPs must be approved for use by DoD information systems in accordance with the process described in Paragraphs 4.2.a. through h. Requests for IdP approvals must be sponsored by an information system owner or DoD Component. Approvals may be reevaluated based on changes to IdP provider capabilities or changes in DoD risk profiles. Information system owners may evaluate IdP solutions in laboratory, test, and development environments to determine if they are suitable for operational use before submitting the IdP for approval. IdP solutions may not be implemented in production environments until approval has been obtained. A full list of approved IdPs is available at https://intelshare.intelink.gov/sites/dodcioicamdocs (permission required).

a. The sponsor will compile:

(1) A description of the IdP, including who operates it, the vendor or vendors providing the solution if applicable, whether any vendors are partially or wholly foreign-owned, what

community of users the IdP supports, and what credential types and authentication actions are supported by the IdP (e.g., PIV public key certificate based authentication or username/password authentication).

(2) A list of the CSPs the IdP validates credentials from, and, if the IdP is also a CSP, how identity proofing is performed prior to issuing credentials.

(3) Documentation on how the IdP ensures the security of its own operations.

(4) How the IdP will meet the requirements identified in Paragraph 3.6.c., including the results from any existing security reviews.

(5) How DoD information systems will be able to authenticate assertions from the IdP (e.g., information about the public key certificate used by the IdP to digitally sign assertions, assertion format, assertion contents, which identifier(s) within the assertion are unique).

(6) Whether users who will be authenticated by the IdP will also be registered using the mission partner registration system to map identifiers provided by the IdP to DoD internally managed identifiers to support identity resolution.

(7) If the IdP is operated by a DoD Component, information regarding the ATO status of the IdP, including any identified risks and planned remediation actions.

b. The sponsor will obtain a memorandum recommending approval from the information system AO or the Component CISO that includes acceptance of risk for using the IdP.

c. The sponsor will submit the required information and recommendation for approval to the DoD CIO ICAM lead.

d. The DoD CIO ICAM lead will coordinate a review of the request with the appropriate governance body as defined by the DoD CIO, and if recommended for approval, request interoperability testing for the IdP from DISA. If disapproved, the DoD CIO ICAM lead will provide the sponsor with the reason the request was disapproved.

e. If existing security review documentation is not sufficient, the DoD CIO ICAM lead may also request a security review of the IdP from the NSA.

f. If interoperability testing is successful and the security review does not identify unacceptable concerns, the DoD CIO ICAM lead will develop a draft approval memorandum that contains applicable guidance including the IAL and AAL that the IdP is approved for and any other restrictions on the use of the IdP.

g. The DoD CIO or delegated DoD Deputy CIO will review the draft approval memorandum and approves or disapproves it.

h. If the request is approved by the DoD CIO, the DoD CIO ICAM lead will provide the approval memorandum to the requestor, and add the approval to the appropriate published list of IdP technology.

i. The DoD CIO ICAM lead will coordinate with DISA as appropriate to develop implementation guidance.

## 4.3. E2P.

The information system owner of information systems that are unable to meet the authentication requirements in Section 3 must obtain an E2P in accordance with the process in Paragraphs 4.3.a. through f. Requests for E2Ps must be sponsored by an information system owner or DoD Component and submitted via the E2P Portal at https://rmfks.osd.mil/dode2p/.

a. The sponsor will compile:

(1) A description of the information system or set of information systems, including justification for why the information system cannot meet the authentication requirements in Section 3, such as constraints on the user community or technical limitations of the information system or its environment.

(2) The desired alternative authentication, including the identity proofing process, authenticator technology, and credential issuance and management processes.

(3) The risk level of the resources that will be accessed using the desired authentication process.

(4) Whether the request is for a permanent use case or a temporary approval. If the request is for a temporary approval, include the expected date the information system or set of information systems will be brought into compliance, or the external dependencies preventing compliance.

b. The sponsor will obtain a recommendation for approval from the information system AO or the Component CISO that includes a vulnerability assessment and acceptance of risk for using the alternative technology and process. The vulnerability assessment must be submitted with the risk acceptance letter.

c. The sponsor will submit the required information and recommendation for approval to the DoD CIO ICAM lead.

d. The DoD CIO ICAM lead will coordinate a review of the request with the appropriate governance body as defined by the DoD CIO, and, if recommended for approval, develops a draft approval memorandum that contains applicable implementation guidance and contact information for the requestor.

e. The DoD CIO will review the request and approves or disapproves it. If approved, the DoD CIO will sign the approval memorandum.

f. If the request is approved by the DoD CIO, the DoD CIO ICAM lead will provide the approval memorandum to the requestor.

# GLOSSARY

## G.1. ACRONYMS.

| ACRONYM | MEANING |
|---|---|
| AAL | authenticator assurance level |
| AO | authorizing official |
| ASCII | American standard code for information interchange |
| ATO | authorization to operate |
| CAC | common access card |
| CIO | chief information officer |
| CISO | chief information security officer |
| COI | community of interest |
| CSO | cloud service offering |
| CSP | credential service provider |
| CUI | controlled unclassified information |
| DDIL | denied, degraded, intermittent, or limited bandwidth |
| DISA | Defense Information Systems Agency |
| DMDC | Defense Manpower Data Center |
| DoDI | DoD instruction |
| DODIN | Department of Defense Information Network |
| DS | defense self-service |
| E2P | exception to policy |
| FAL | federation assurance level |
| FIPS | Federal Information Processing Standard |
| IAL | identity assurance level |
| ICAM | identity, credential, and access management |
| IdP | identity provider |
| IL | impact level |
| IT | information technology |
| JPIO | Joint Program Integration Office |
| MFA | multi-factor authentication |
| NIAP | National Information Assurance Partnership |
| NIPRNET | Non-classified Internet Protocol Router Network |
| NIST | National Institute of Standards and Technology |
| NPE | non-person entity |
| NSA | National Security Agency |

| ACRONYM | MEANING |
|---|---|
| PII | personally identifiable information |
| PIV | personal identity verification |
| PKI | public key infrastructure |
| RPA | robotic process automation |
| SAP | special access program |
| SIPRNET | SECRET Internet Protocol Router Network |
| SP | special publication |
| SRG | security requirements guide |
| SSH | Secure Shell |
| TLS | transport layer security |
| USD(I&S) | Under Secretary of Defense for Intelligence and Security |
| USD(P&R) | Under Secretary of Defense for Personnel and Readiness |

## G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

| TERM | DEFINITION |
|---|---|
| **Assertion** | Defined in DoD Enterprise ICAM Reference Design. |
| **assurance level** | Defined in DoD Enterprise ICAM Reference Design. |
| **Authentication** | Defined in DoD Enterprise ICAM Reference Design. |
| **Authenticator** | Defined in DoD Enterprise ICAM Reference Design. |
| **Beneficiary** | Defined in DoD Enterprise ICAM Reference Design. |
| **Credential** | Defined in DoD Enterprise ICAM Reference Design. |
| **CSP** | Any DoD Component, COI, or local information system that issues its own credentials. |
| **Designee** | An individual who is designated to represent a beneficiary, either by the beneficiary themselves or through a legal process such as dependency or power of attorney. |
| **digital identity** | Defined in DoD Enterprise ICAM Reference Design. |

| TERM | DEFINITION |
|---|---|
| **Entitlement** | Defined in DoD Enterprise ICAM Reference Design. |
| **Entity** | Defined in DoD Enterprise ICAM Reference Design. |
| **FAL** | Defined in DoD Enterprise ICAM Reference Design. |
| **functional privileged user** | Defined in DoD Enterprise ICAM Reference Design. |
| **hardware public key certificate** | A public key certificate where the associated private key is established and stored in a Level 3 hardware validated cryptographic module. |
| **Hash** | A function that maps a set of characters to another set of characters such that it is computationally infeasible to determine the original set and such that two different sets of characters will have different hash values. |
| **high impact** | Defined in NIST FIPS 199. |
| **IAL** | Defined in DoD Enterprise ICAM Reference Design. |
| **identity proofing** | Defined in DoD Enterprise ICAM Reference Design. |
| **IdP** | Defined in DoD Enterprise ICAM Reference Design. |
| **Identity** | Defined in DoD Enterprise ICAM Reference Design. |
| **information system** | Defined in DoD Enterprise ICAM Reference Design. |
| **IT privileged user** | Defined in DoD Enterprise ICAM Reference Design. |
| **low impact** | Defined in NIST FIPS 199. |
| **mission partner** | Defined in DoD Enterprise ICAM Reference Design. |
| **MFA** | Defined in DoD Enterprise ICAM Reference Design. |
| **moderate impact** | Defined in NIST FIPS 199. |
| **NPE** | Defined in DoD Enterprise ICAM Reference Design. |
| **person entity** | Defined in DoD Enterprise ICAM Reference Design. |

| TERM | DEFINITION |
|---|---|
| **privileged user** | Defined in DoD Enterprise ICAM Reference Design. |
| **public key certificate** | Defined in DoD Enterprise ICAM Reference Design. |
| **PKI** | Defined in DoD Enterprise ICAM Reference Design. |
| **Resource** | Defined in Committee on National Security Systems Instruction 4009. |
| **requirements definition** | Act of documenting and verifying condition or capability needed by a user to meet mission needs. |
| **Salt** | A random number generated prior to hashing a password to ensure uniqueness and prevent reverse attacks. |
| **sensitivity level** | To express how the risk of unauthorized access or unauthorized dissemination will impact DoD missions or business processes using that data. Sensitivity levels have been replaced by risk levels in this issuance. |
| **software public key certificate** | A public key certificate where the associated private key is established and stored in a Level 1 validated cryptographic module. |
| **virtual device** | An application that can emulate a physical device, or provide functionality like that provided by a physical device without emulating any specific physical device. |
| **virtual machine** | A computer system created using software on one physical computer in order to emulate the functionality of another separate physical computer |

# REFERENCES

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Committee on National Security Systems Policy No. 11, "Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products," current edition

Department of Defense Cloud Computing Security Requirements Guide (SRG), March 6, 2017

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, June 2020[1]

DoD Identity, Credential, and Access Management (ICAM) Strategy, March 30 2020

DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," January 23, 2014, as amended

DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program," March 2, 2016

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems ," July 19, 2022

DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

Executive Order 12333, "United States Intelligence Activities," December 4, 1981

Memorandum of Agreement between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 17, 2017

National Information Assurance Partnership "Protection Profile Module for SSL/TLS Inspection Proxy," August 23, 2019

National Institute of Standards and Technology Federal Information Processing Standard (FIPS) 140-3, "Security Requirements for Cryptographic Modules," March 22, 2019

National Institute of Standards and Technology Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

National Institute of Standards and Technology Federal Information Processing Standard (FIPS) 201-2, "Person Identity Verification (PIV) of Federal Employees and Contractors," August 2013

[1] Available at https://dodcio.defense.gov/Library/

National Institute of Standards and Technology Special Publication 800-131A, "Transitioning the Use of Cryptographic Algorithms and Key Lengths," March 2019

National Institute of Standards and Technology Special Publication 800-63-3, "Digital Identity Guidelines," June 22, 2017, as amended

National Institute of Standards and Technology Special Publication 800-63A, "Enrollment and Identity Proofing" June 2017, as amended

National Institute of Standards and Technology Special Publication 800-63B, "Authentication and Lifecycle Management" June 2017, as amended

United States Department of Defense Web Content Filter X.509 Certificate Policy, October 10, 2019