Unit #8

MIS 5214

Access Control

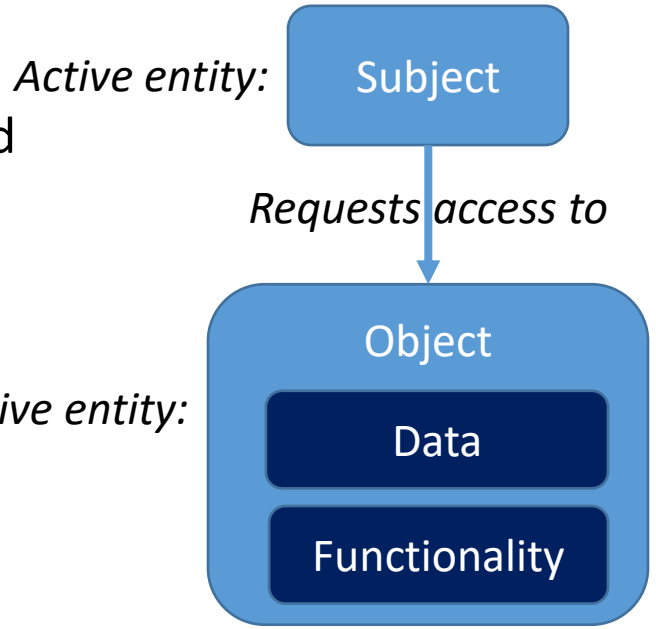
Agenda

- Access Control
- Identification and Authentication
  - Digital Identity Guidelines
- Centralized Remote Access Control Technologies

Access

The flow of information between a subject and an object

- Subject
  - Is an active entity that requests access to an object or the data within the object
  - Can be a user, program, or process
- Object
  - Can be a computer, computer directory, file, program, database or field within a table within a database

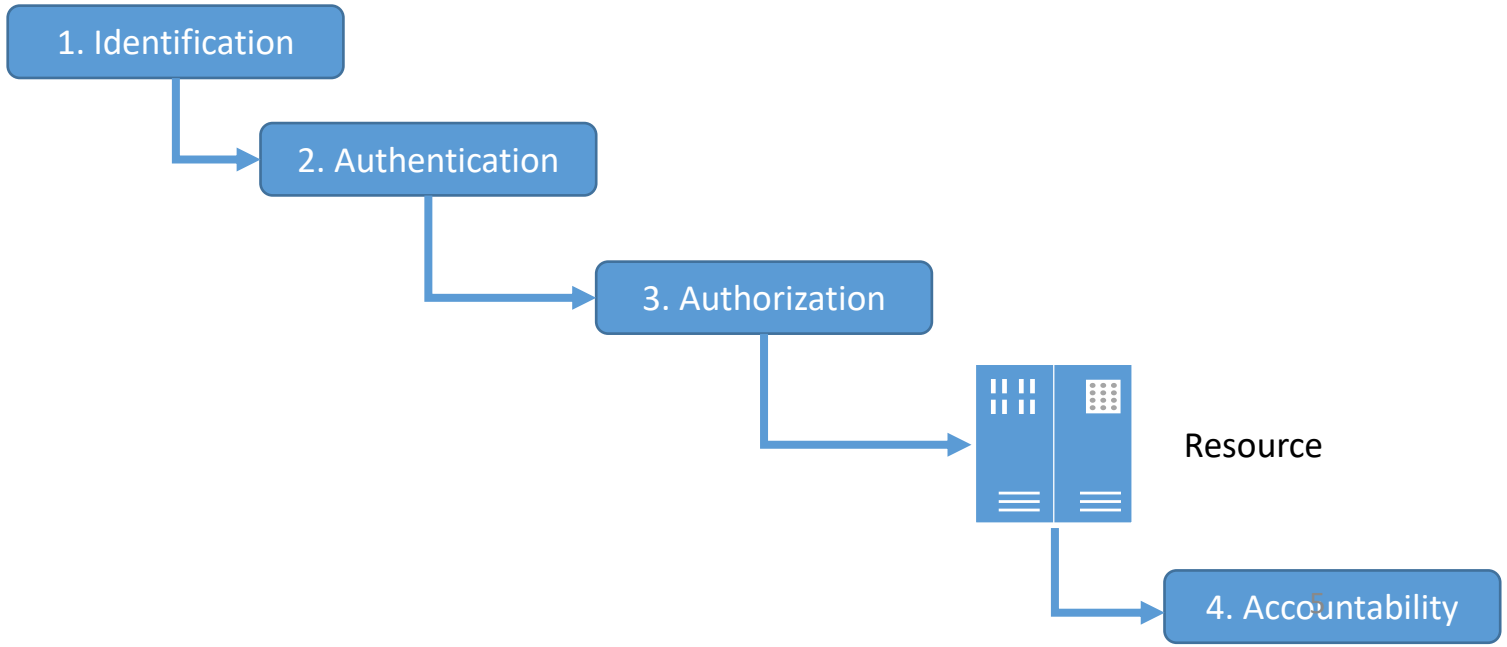


Access Controls

- Broad term covering several types of mechanisms that control access to features of networks, computers and information stored and flowing within them
- First line of defense in battling unauthorized access to network resources and systems
  - Give organizations ability to control, restrict, monitor and protect resource confidentiality, integrity and availability

Identification, Authentication, Authorization, and Accountability

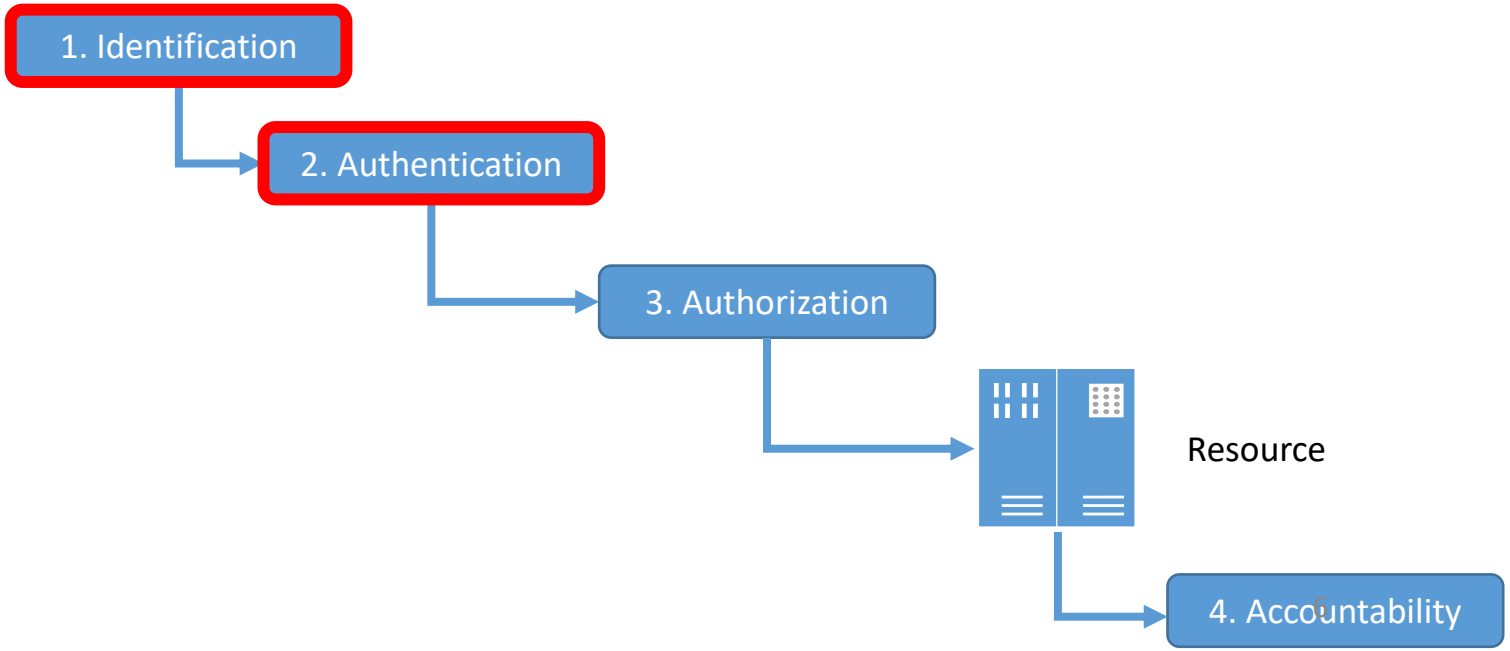
To access a network's resource, a user must:



Identification, Authentication, Authorization, and Accountability

To access a network's resource, a user must:

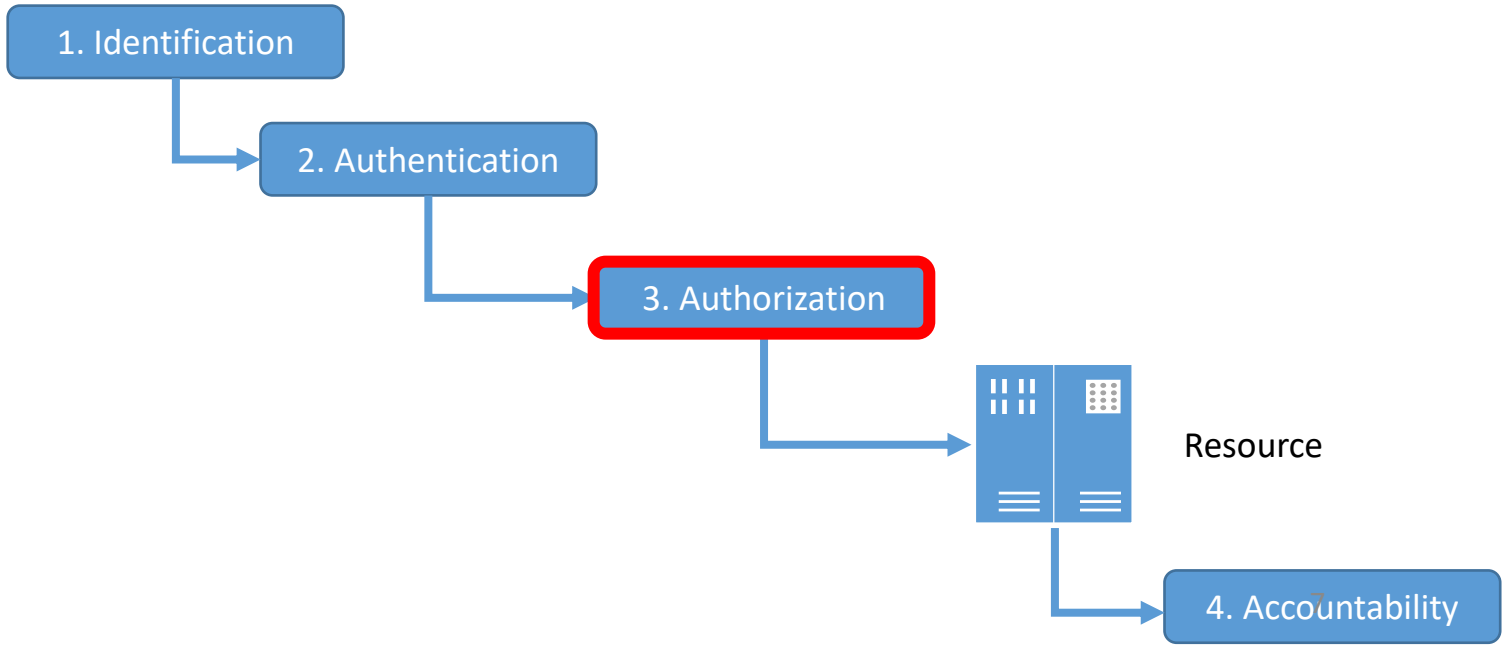
- **Prove their identity (i.e. has the necessary credentials)**



Identification, Authentication, Authorization, and Accountability

To access a network's resource, a user must:

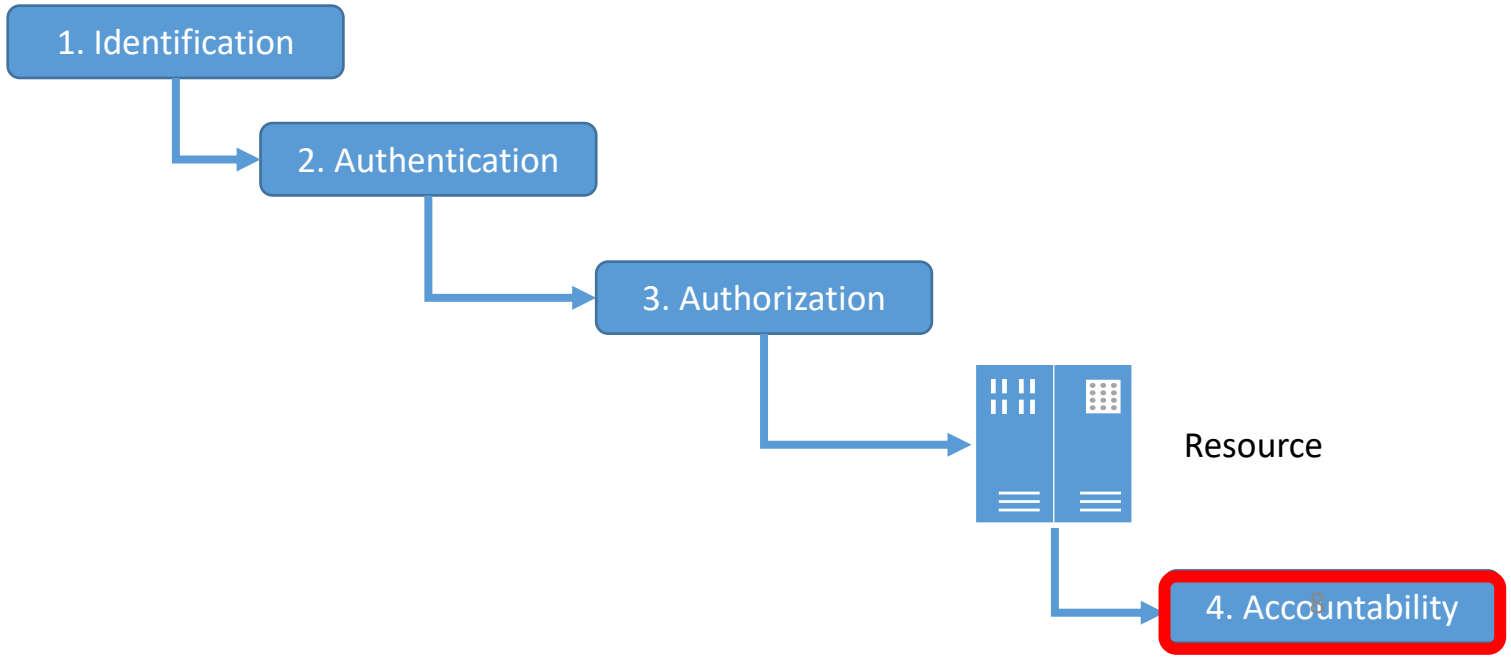
- Prove their identity (i.e. has the necessary credentials),
- **Have been given privileges to access a resource and perform action they are requesting**



Identification, Authentication, Authorization, and Accountability

To access a network's resource, a user must:

- Prove their identity (i.e. has the necessary credentials),
- Have been given privileges to access a resource and perform action they are requesting
- **Be tracked to enforce accountability of their actions**

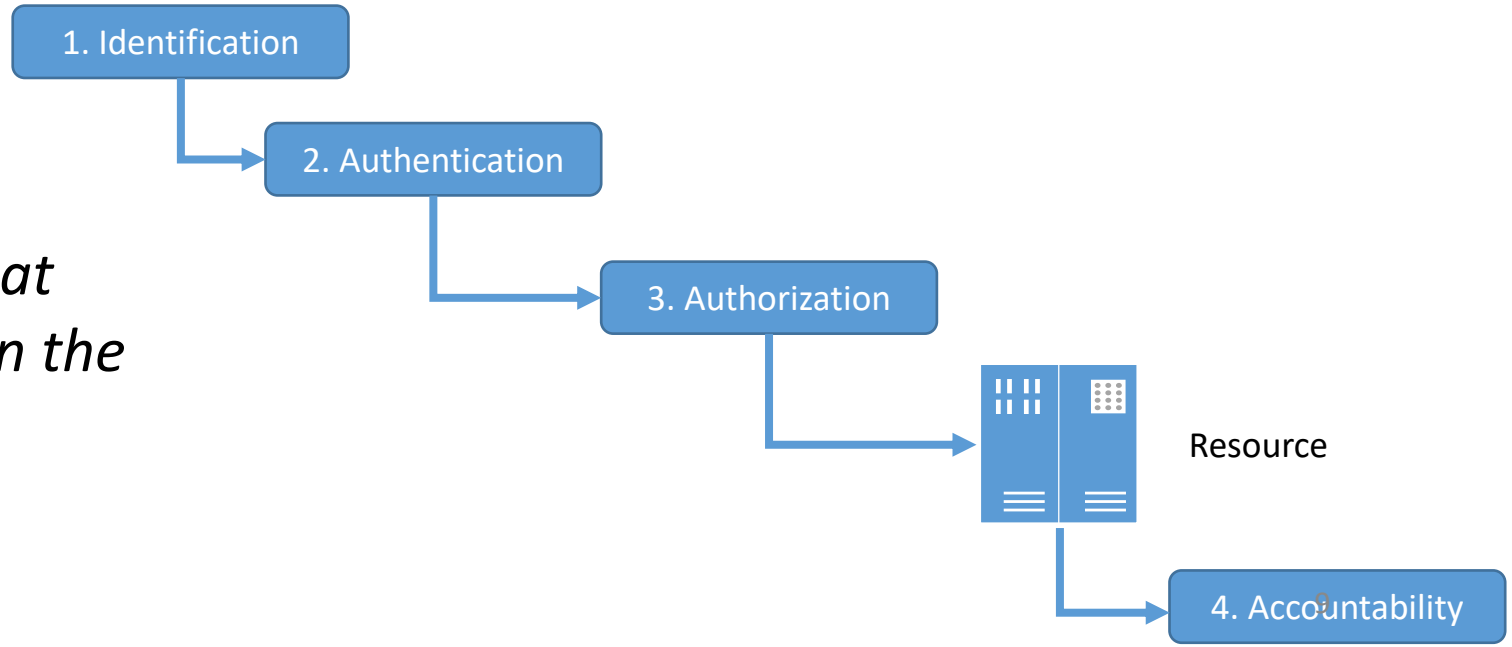


Identification, Authentication, Authorization, and Accountability

To access a network's resource, a user must:

- Prove their identity (i.e. has the necessary credentials),
- Have been given privileges to perform action they are requesting
- Be tracked to enforce accountability of their actions

Each has distinct functions that fulfill a specific requirement in the process of access control



Logical Access Controls

- Are technical tools used for identification, authentication, authorization and accountability
  - “Logical” and “Technical” are synonyms that can be used interchangeably in this context
- Can be embedded in operating systems, applications, add-on security packages, databases and telecommunication management systems

Identification and Authentication

Usually involves a two-step process:

1. **Identification:** Entering public information
   - Method by which a subject (user, program or process) claims to have a specific identity
     - *Username, employee number, account number, or email address*

2. **Authentication:** Entering private information
   - Individual's identify must be verified during authentication process
   - Method by which subject proves it is who it says it is
     - *Static password, smart authenticator ("token"), one-time password, or PIN*

Identification

Identification: Entering public information

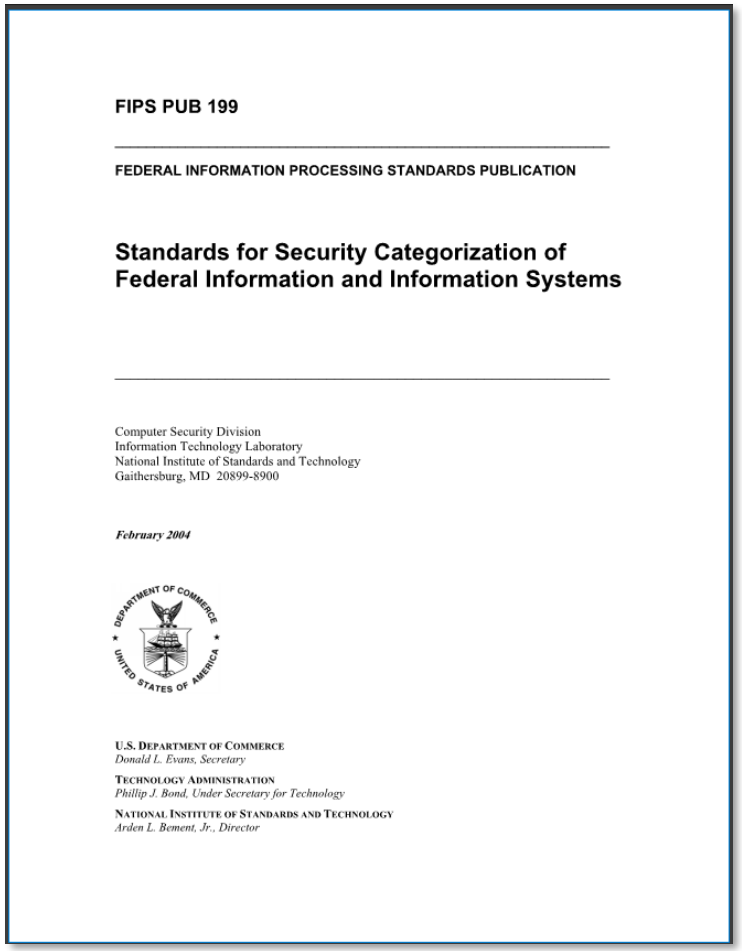
- Method by which a subject (user, program or process) supplies identifying information to claim they have a specific identity
  - *Username, employee number, account number, or email address*

- Creating secure identities involves 3 key aspects:
  1. **Uniqueness** – every user, program or process must be identified with an identifier (i.e. unique ID) that is specific to the individual for accountability
  2. **Non-descriptive** – Identifier should not indicate the purpose of the account nor the user's position nor tasks done with the account
  3. **Issuance** – provided by an authority as a formal/official means of proving identity

Question:

How should information systems be set up to control CIA breach risks to their data content?

FIPS 199: Risk assessment based on security objectives and impact ratings



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

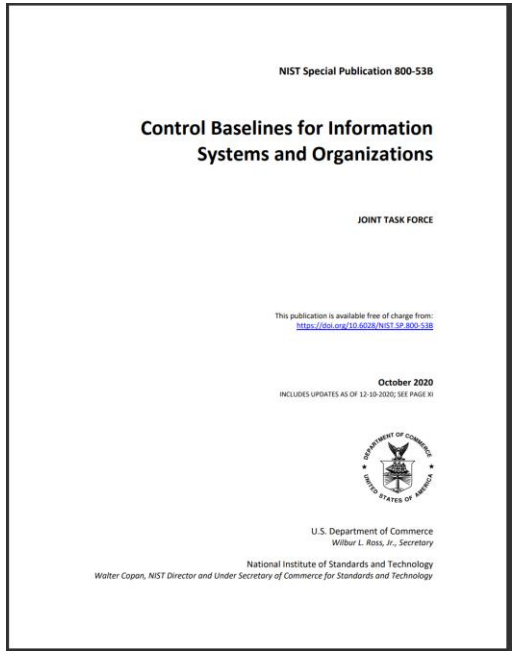
February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.


NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53B

October 2020

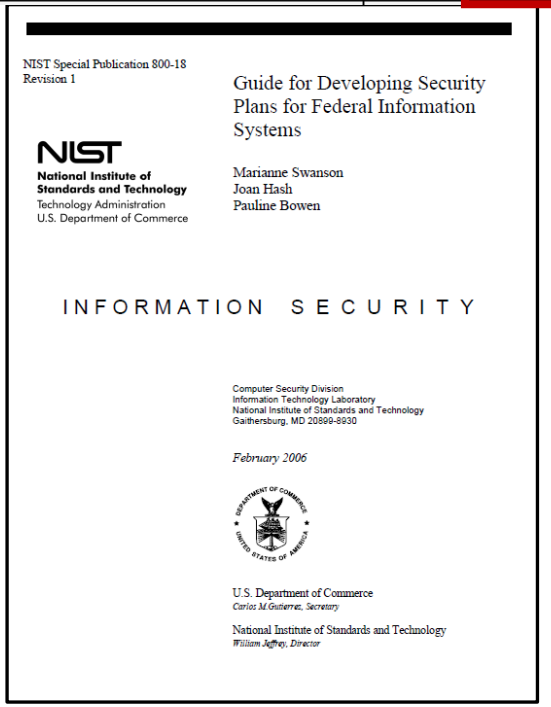
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Identification and Authentication			Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC


NIST Special Publication 800-18 Revision 1

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

INFORMATION SECURITY

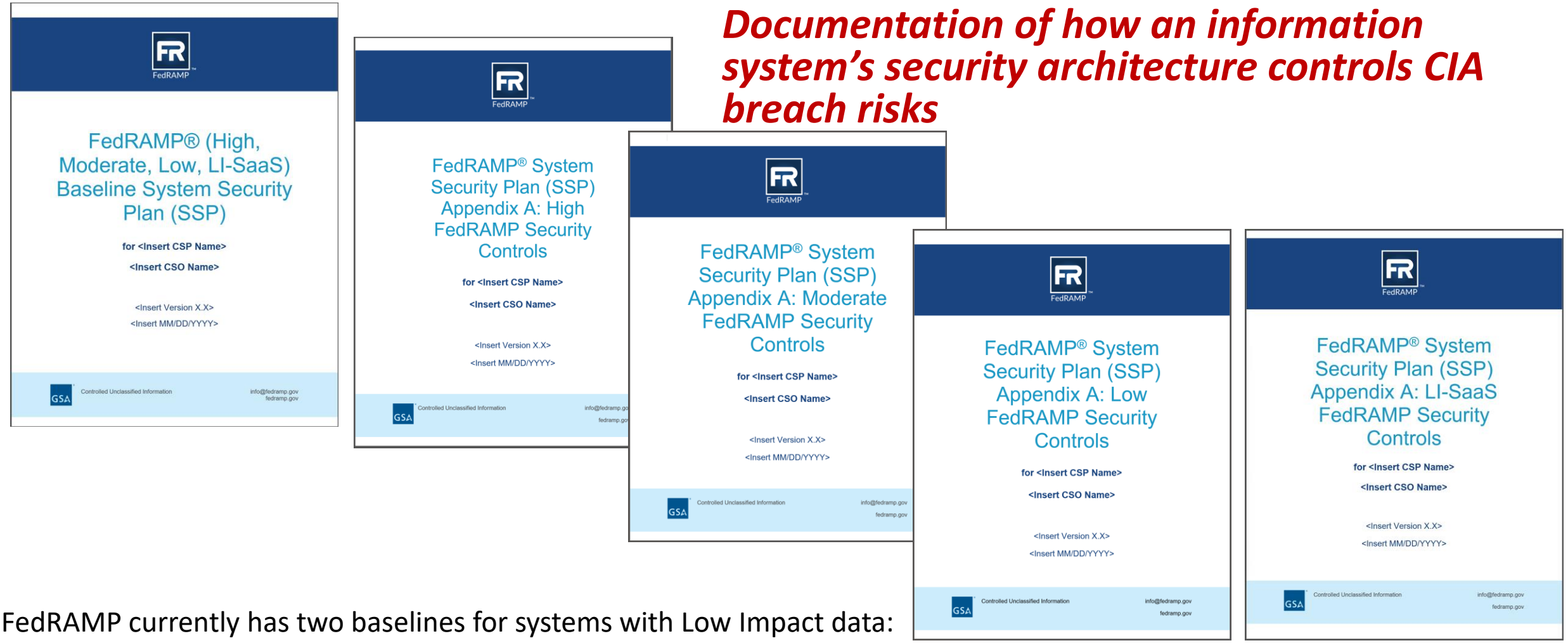
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

Documentation of how an information system's security architecture controls CIA breach risks



FedRAMP currently has two baselines for systems with Low Impact data:

- Low Baseline
- "Tailored" LI-SaaS Baseline
  - Accounts for Low-Impact SaaS applications that do not store personal identifiable information (PII) beyond that generally required for login capability (i.e. username, password, and email address). Required security documentation is consolidated and the requisite number of security controls needing testing and verification are lowered relative to a standard Low Baseline authorization.

FedRAMP

FedRAMP® System Security Plan (SSP) Appendix A: High FedRAMP Security Controls

for <Insert CSP Name>

<Insert CSO Name>

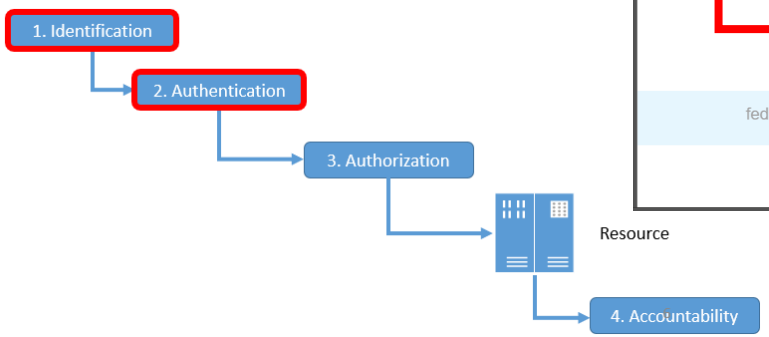
<Insert Version X.X>

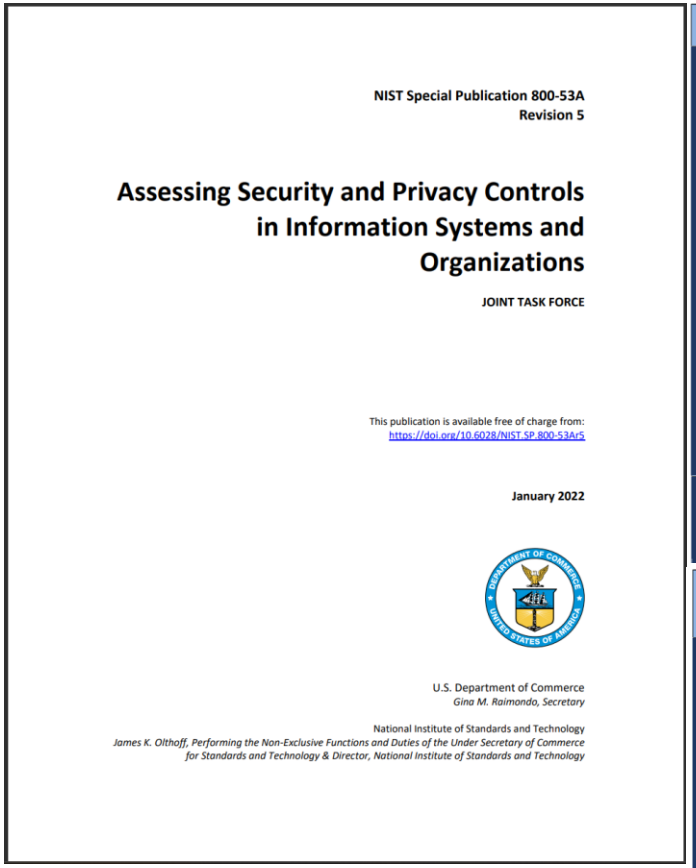
<Insert MM/DD/YYYY>

GSA Controlled Unclassified Information

info@fedramp.gov

fedramp.gov





NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

IA-02	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02[01]	organizational users are uniquely identified and authenticated;
	IA-02[02]	the unique identification of authenticated organizational users is associated with processes acting on behalf of those users.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; organizational personnel with account management responsibilities; system developers].
	IA-02-Test	[SELECT FROM: Organizational processes for uniquely identifying and authenticating users; mechanisms supporting and/or implementing identification and authentication capabilities].

IA-02(01)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(01)	multi-factor authentication is implemented for access to privileged accounts.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(01)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(01)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing a multi-factor authentication capability].

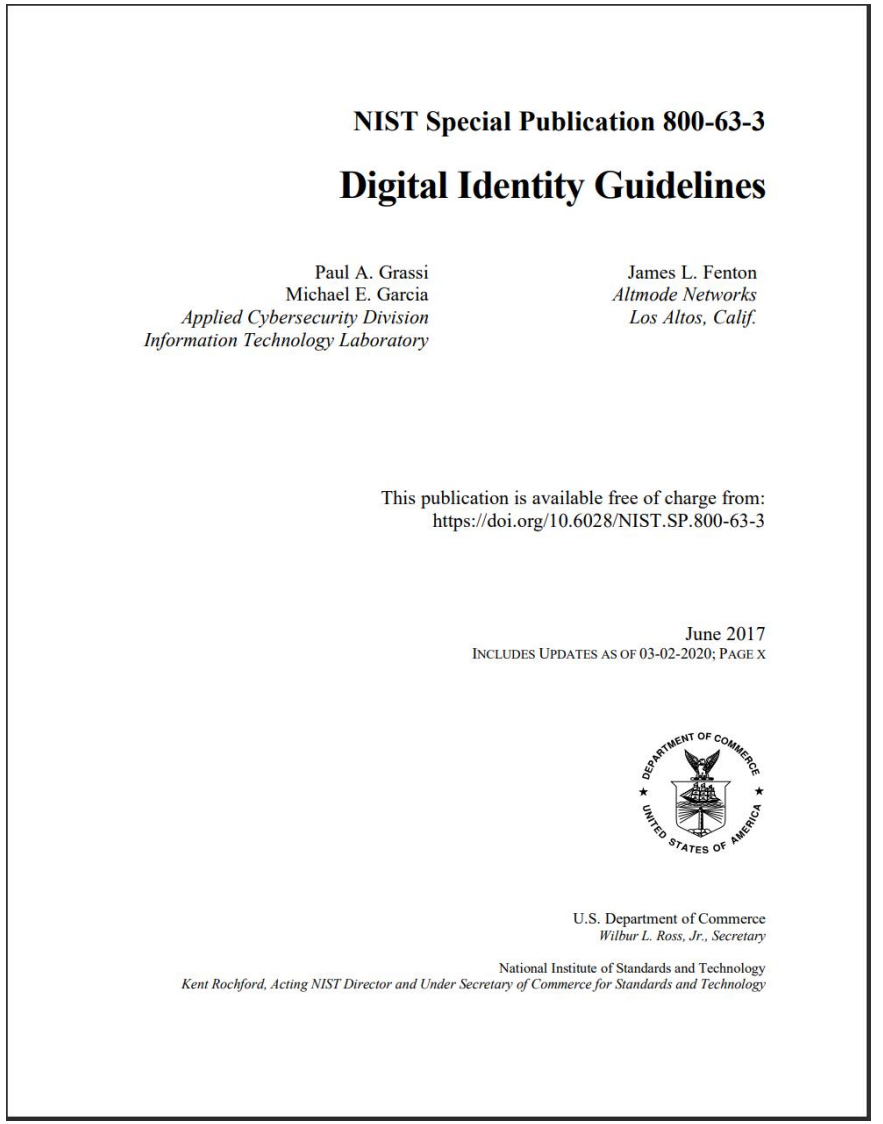
How should information systems identify and authenticate users, programs, and processes to control risks to the CIA of their data content?

IA-02(02)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(02)	multi-factor authentication for access to non-privileged accounts is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(02)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(02)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing a multi-factor authentication capability].

NIST 800 63-3: Digital Identity Guidelines

Controls focus on 2 errors we seek to avoid:

1. **The impact of providing a service to the wrong subject**
   - E.g. An attacker successfully identifies as someone else
2. **The impact of excessive identity proofing**
   - I.e. collecting and storing more information about a person than is required to successfully provide the digital service



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

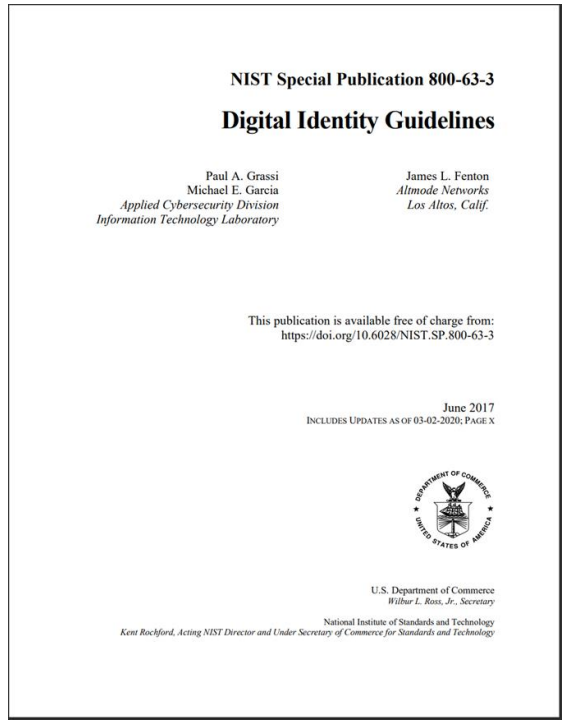
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
INCLUDES UPDATES AS OF 03-02-2020; PAGE X

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Digital Identity Guidelines



NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
INCLUDES UPDATES AS OF 03-02-2020; PAGE X

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

6 Categories of impact resulting from providing a service to the wrong subject

1. Inconvenience, distress, or damage to standing or reputation
2. Financial loss or agency liability
3. Harm to agency programs or public interests
4. Unauthorized release of sensitive information
5. Personal safety
6. Civil or criminal violations

Identity and Authentication Controls are selected based on information security breach impact levels:

1. Low impact
2. Moderate impact
3. High impact

Impact-based determination of Identity and Authentication Assurance Levels

Table 6-1 Maximum Potential Impacts for Each Assurance Level

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

Agenda

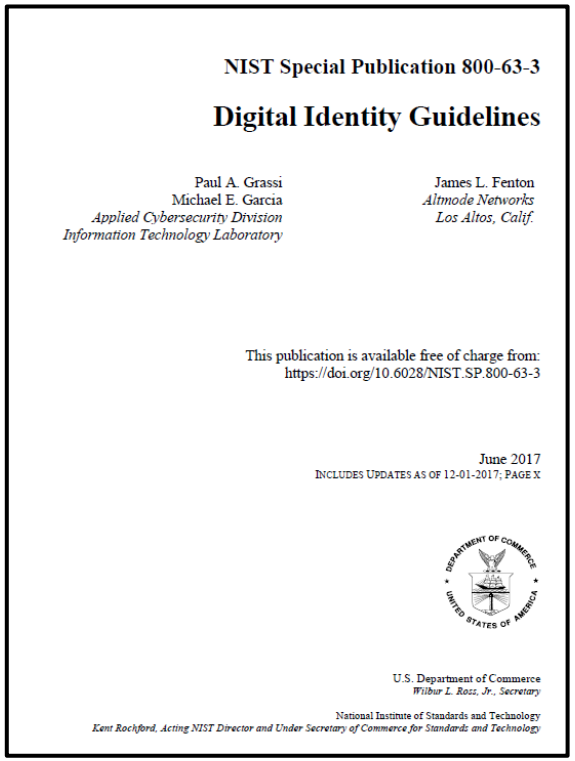
- ✓New schedule for today's classes and mid-term exam
- ✓Access Control
- Identification and Authentication
  - Digital Identity Guidelines
  - Biometrics (quick overview/review)
- Centralized Remote Access Control Technologies

Identity & Authentication Assurance Levels are defined as:

1. The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued
   - **IAL – Identity Assurance Level**

2. The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued
   - **AAL – Authentication Assurance Level**

Digital Identity & Authentication Guidelines


NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
INCLUDES UPDATES AS OF 12-01-2017; PAGE X

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Specifies **3 kinds of identity authentication assurance controls to select in** mitigating risks associated with impacts resulting from identity and authentication errors in electronic transactions:

1. *Enrollment and Identity Proofing*
   - Protecting against: A false claim to an identity
2. *Authentication and Lifecycle Management*
   - Protecting against: A false use of a credential
3. *Federation and Assertions*
   - A false or compromised identity passed among a collection of systems
   - NIST SP 800-63C

Identity Assurance Credentials

Verifiers use credentials to authenticate the Claimant's identity based on possession and control of the corresponding authenticator

- Paper credentials presented by subject in-person can be checked to verify that the physical holder of the credential is the subject, these include:
  - Passports, birth certificates, driver's licenses, employee identity cards…
- Verification of electronic credentials
  - The password database entries possessed by the Verifier are considered to be the credentials
  - Public key certificates (X.509) are a classic example of credentials the Claimant can possess
  - To authenticate a Claimant using an electronic credential, the Verifier validates the credential and assures it was issued by an authorized Credential Service Provider and has not expired or been revoked by
    1. Determining if the credential has been signed by the Credential Service Provider
    2. Interactively querying the Credential Service Provider through a secure protocol

Identity Assurance

NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing

Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

Privacy Authors:
Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Jamie M. Danker
National Protection and Programs Directorate
Department of Homeland Security

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Information Access Division
Information Technology Laboratory

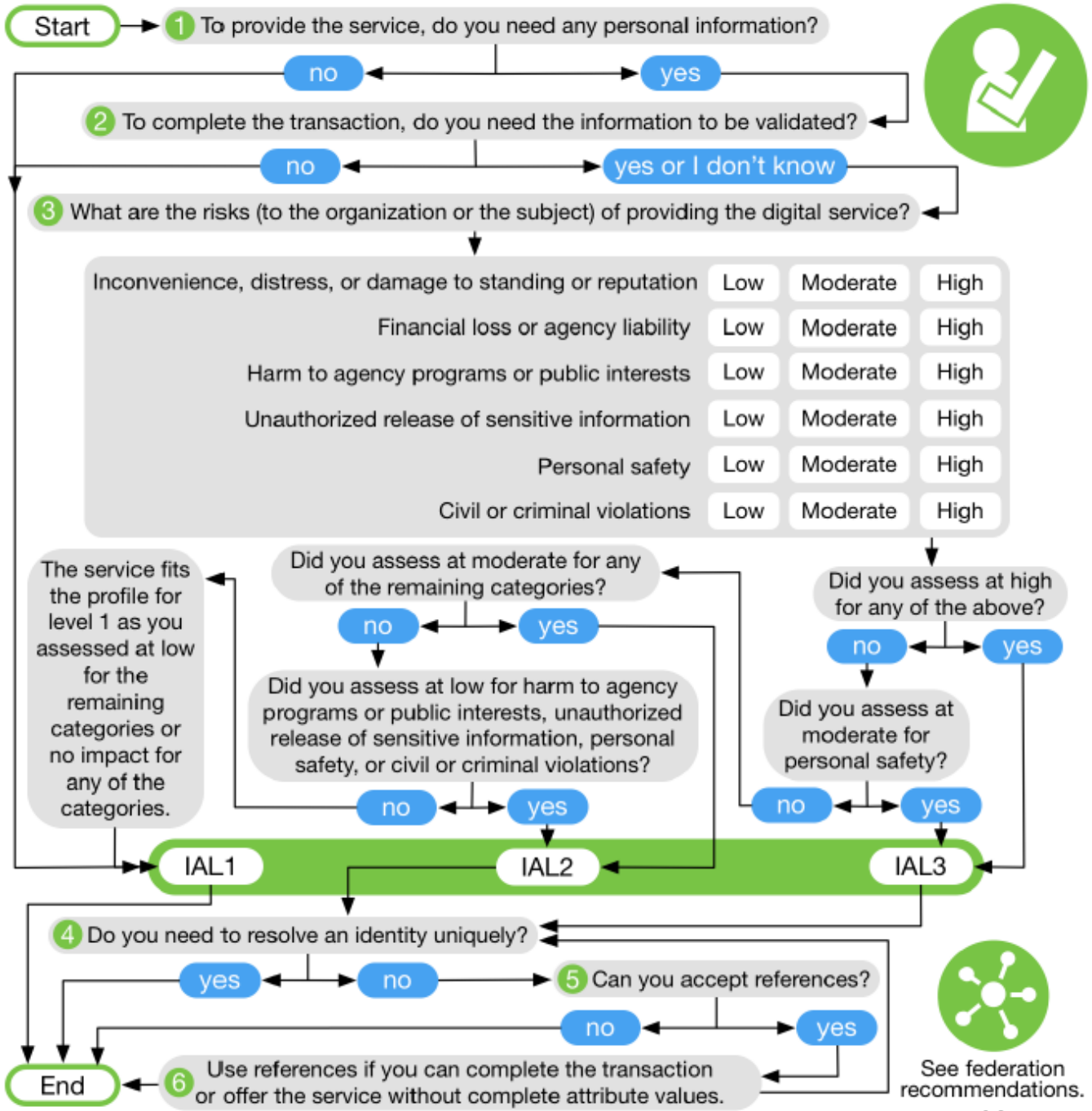
Mary F. Theofanos
Office of Data and Informatics
Material Measurement Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a

June 2017
INCLUDES UPDATES AS OF 12-01-2017; PAGE VII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

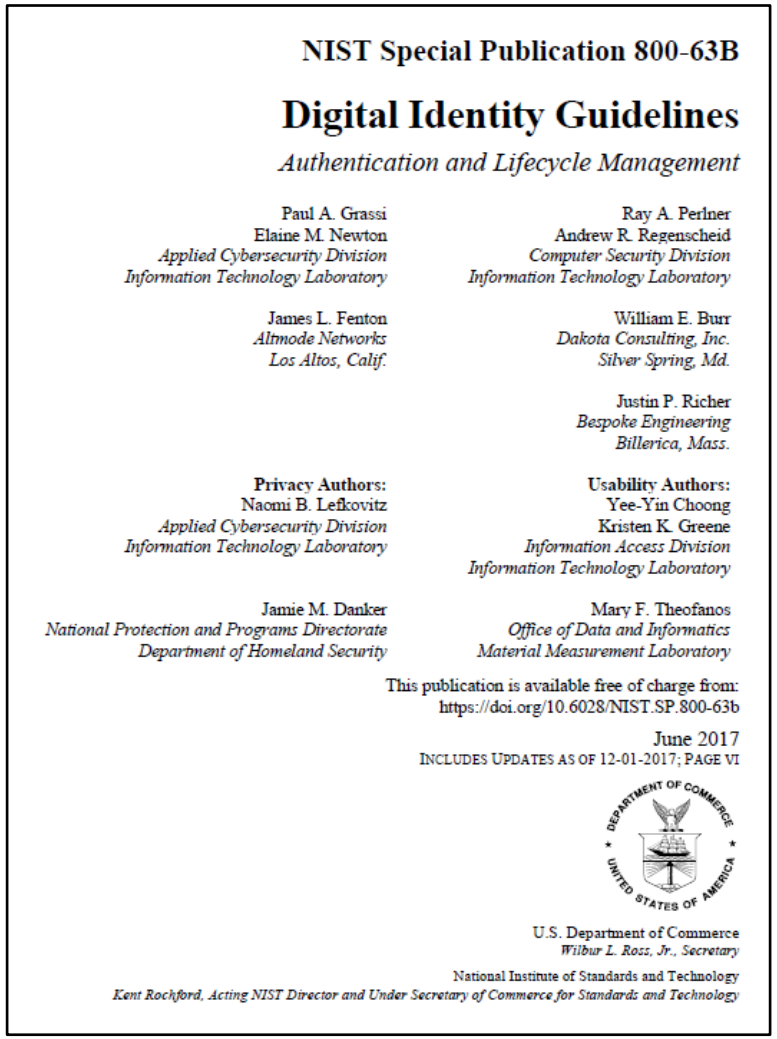


Identity Assurance

Identity Assurance Level
IAL1: At IAL1, attributes, if any, are self-asserted or should be treated as self-asserted.
IAL2: At IAL2, either remote or in-person identity proofing is required. IAL2 requires identifying attributes to have been verified in person or remotely using, at a minimum, the procedures given in SP 800-63A.
IAL3: At IAL3, in-person identity proofing is required. Identifying attributes must be verified by an authorized CSP representative through examination of physical documentation as described in SP 800-63A.

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2

Authentication Assurance



NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
Elaine M. Newton
Applied Cybersecurity Division
Information Technology Laboratory

Ray A. Perlner
Andrew R. Regenscheid
Computer Security Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

William E. Burr
Dakota Consulting, Inc.
Silver Spring, Md.

Justin P. Richer
Bespoke Engineering
Billerica, Mass.

Privacy Authors:
Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Information Access Division
Information Technology Laboratory

Jamie M. Danker
National Protection and Programs Directorate
Department of Homeland Security

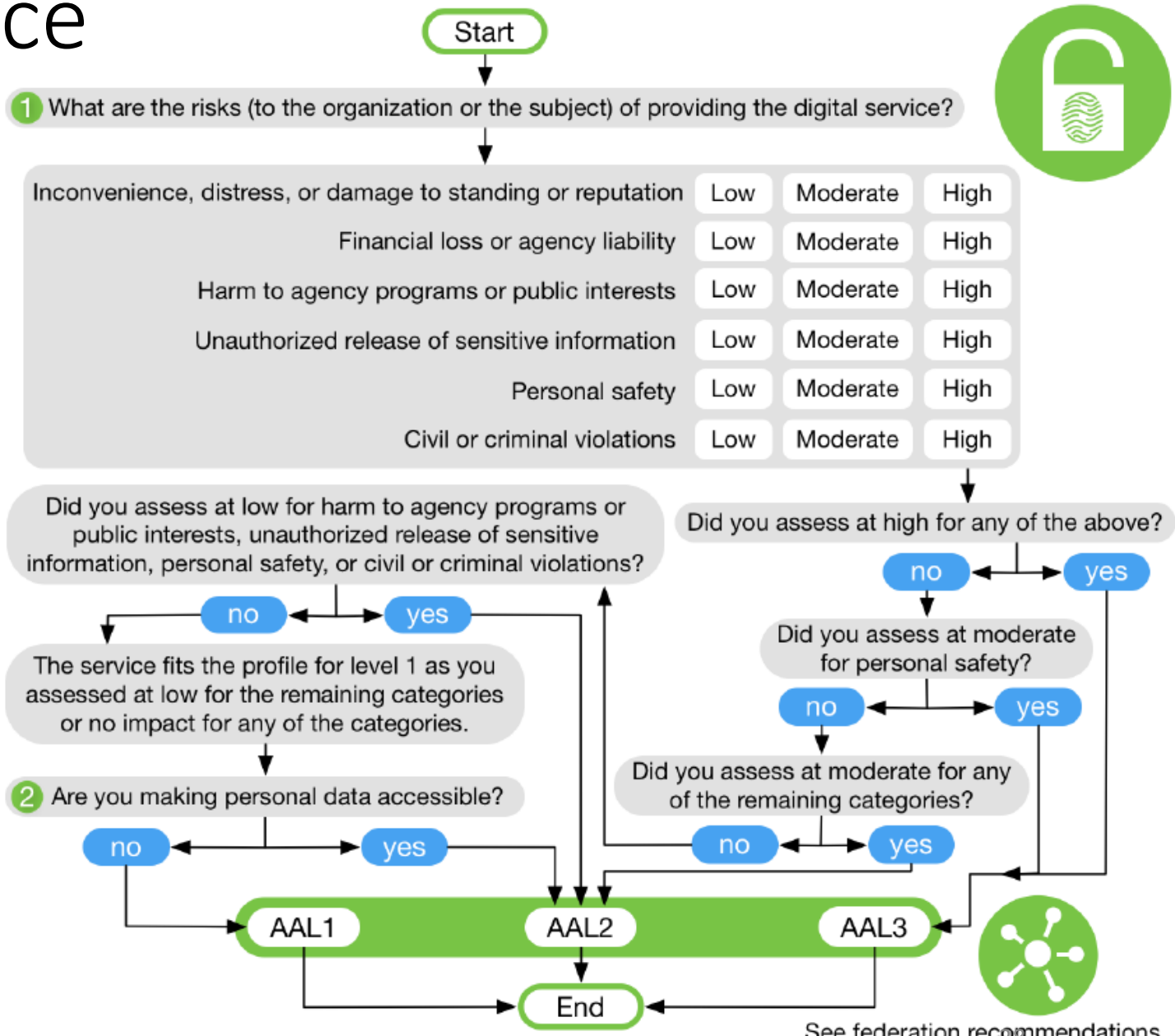
Mary F. Theofanos
Office of Data and Informatics
Material Measurement Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

June 2017
INCLUDES UPDATES AS OF 12-01-2017; PAGE VI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology



Authenticator Assurance

Authenticator Assurance Level
AAL1: AAL1 provides some assurance that the claimant controls an authenticator registered to the subscriber. 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.
AAL2: AAL2 provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above.
AAL3: AAL3 provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a "hard" cryptographic authenticator that provides verifier impersonation resistance.

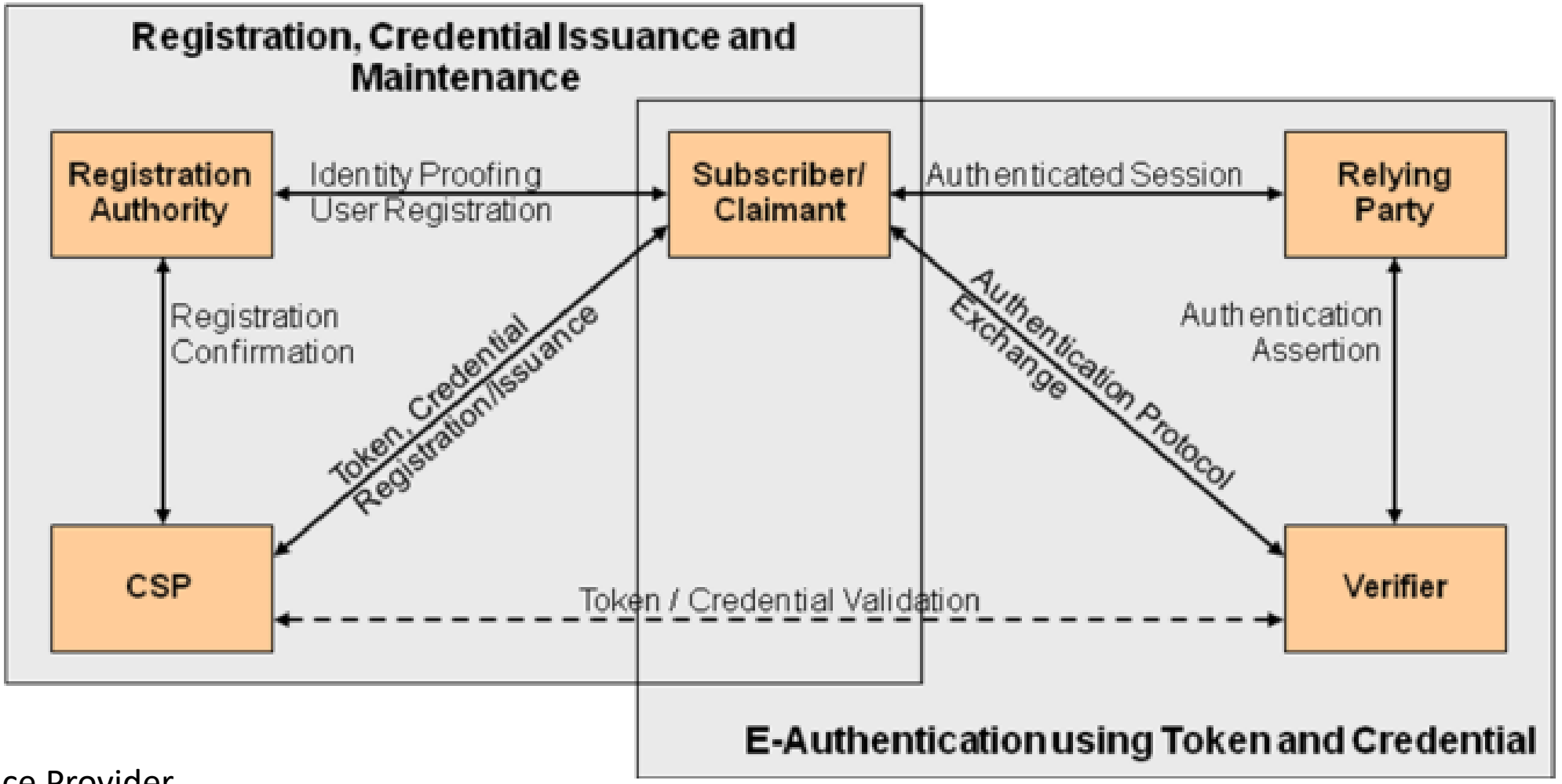
Each assurance level describes the degree of certainty that the user has presented an identifier that refers to his or her identity

Assurance is defined as:

1. The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued
2. The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Identity Assurance levels:

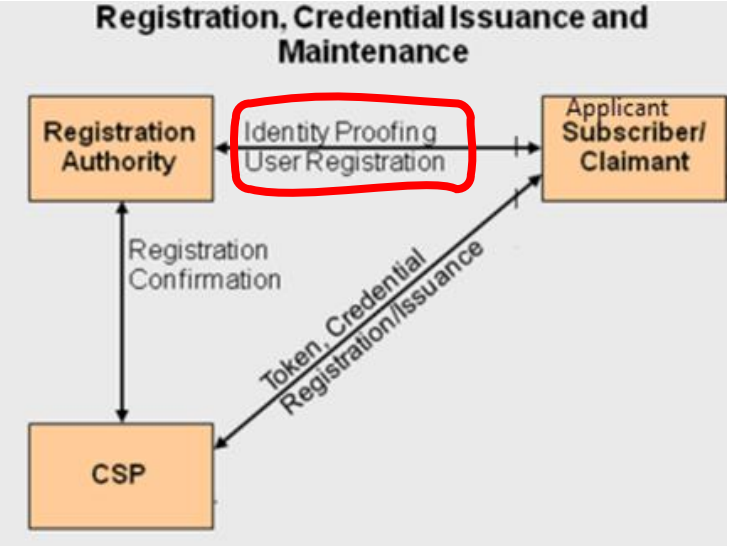
1. **Level 1**: Little or no confidence in the asserted identity's validity
2. **Level 2**: High confidence in the asserted identity's validity
3. **Level 3**: Very high confidence in the asserted identity's validity



CSP = Credential Service Provider

Figure 1 - *The NIST SP 800-63-1 E-Authentication Architectural Model*

Identity Assurance Levels



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

Requirement	IAL1	IAL2	IAL3
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence, **OR** • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, **OR** • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2
Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.
Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	• SP 800-53 • Moderate Baseline (or equivalent federal or industry standard).	• SP 800-53 • High Baseline (or equivalent federal or industry standard).

Authentication – Classic 3 factor paradigm

…for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

1. **Something the subject knows** (“authentication by knowledge”)
   - Examples: password, PIN, combination to a lock…
   - Usually least expensive method to implement
   - Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. **Something the subject has** (“authentication by ownership”)
   - Examples: Key, swipe card, access card, badge…
   - Common for accessing facilities, sensitive areas, and authenticate holder
   - Vulnerability: Can be lost or stolen and result in unauthorized access

3. **Something the subject is** (“authentication by characteristic”)
   - Examples: Fingerprint, palm scan, retina scan…
   - Based on biometrics – a way to identify the subject by a unique physical attribute
   - Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection

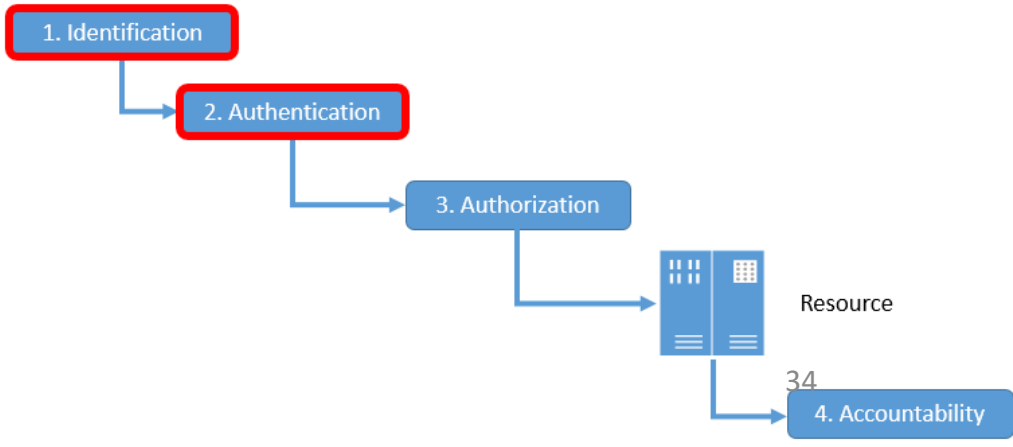
Authentication

Multi-factor authentication refers to use of >1 factor

- Something the subject knows ("authentication by knowledge")
- Something the subject has ("authentication by ownership")
- Something the subject is ("authentication by characteristic")

Authentication system strength determined by the number of factors incorporated into the systems

- 2 factor implementations considered stronger than those using 1 factor
- Systems that incorporate 3 factors are stronger than 2 factor systems



E-Authentication is slightly different from "classic" authentication

E-authenticators always contain a secret

- Used by the claimant to prove possession and control of the authenticator

Some of the classic authentication factors do not apply directly to e-authentication, for example:

- ID badge is "something you have" useful for authenticating to a human (e.g. a guard), but is not usually an authenticator for e-authentication
- Authentication factors classified as "something you know" are not necessary secrets
  - *Knowledge based authentication where a claimant is prompted to answer questions that can be confirmed from public databases does not constitute an acceptable secret for e-authentication*

E-Authentication, is slightly different from “classic” authentication

- Claimant authenticates to a system or application over a network by proving that he/she has possession and control of an authenticator registered with the Credential Service Provider for proving the bearer’s identity
- *The authenticator contains a secret the Claimant uses to prove that he/she is the Subscriber named in a particular credential*
  - The authenticator uses the secret to generate an output (“token”)

    …used in the authentication process to demonstrate and prove the Claimant is the person to whom the authenticator was issued

E-Authentication Authenticators –

The secret contained in a is based on either public/private key pairs (asymmetric keys) or a shared authenticator secret (symmetric key)

Public Key authenticators - have the private key stored in the authenticator

A Verifier knowing the Claimant's public key through some credential (typically a public key certificate) can use an authentication protocol to verify the Claimant's identity, by proving that the Claimant has possession and control of the associated private key authenticator

- **Shared Secret authenticators** – may be either symmetric keys or passwords
  - While often used in similar protocols, an important difference is how they related to the Subscriber
    - **Symmetric keys** are stored in hardware or software that the Subscriber controls
      - ***"Something the Subscriber has"***
    - **Passwords** are memorized by the Subscriber
      - ***"Something the Subscriber knows"***
      - *More vulnerable to password guessing network attacks, keyboard logging, and being learned by someone watching the password being entered than practical for cryptographic keys*
        - *Also susceptible to keyboard logging*

Either way - Subscriber has a duty to maintain exclusive control of his/her authenticator, since possession and control of the authenticator is used to authenticate the Claimant's identity

Assertions

On completion of the authentication process, the Verifier generates an assertion containing the result of the authentication and provides it to the RP

- Examples of Assertions:
  - Cookies – Character strings, placed in memory, which are available to websites within the same Internet domain as the server that placed them in the Web browsers. Cookies may be assertions or pointers to assertions
  - SAML (Security Assertion Markup Language) Assertions – Specified using a mark-up language intended for describing security assertions. They can be used by a Verifier to make a statement to a RP about the identity of a Claimant, and may be digitally signed
  - Kerberos Tickets – Allow a ticket granting authority to issue session keys to tow authenticated parties using symmetric key based encapsulation schemes

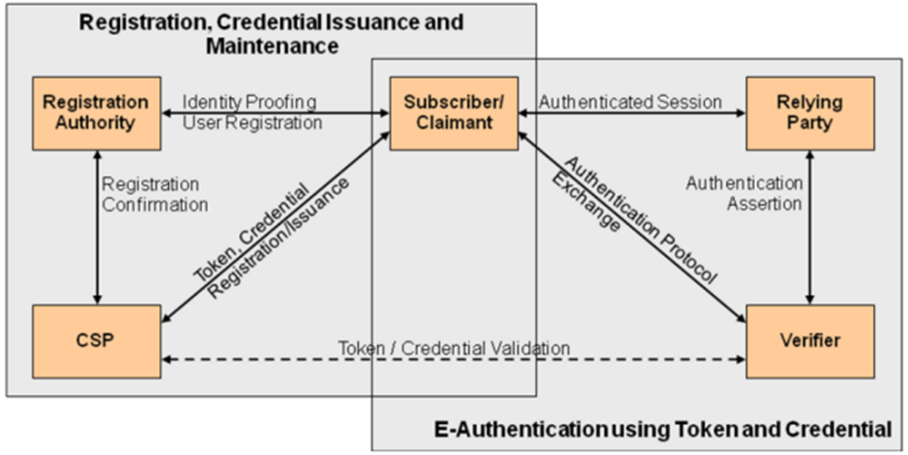


Figure 1 - *The NIST SP 800-63-1 E-Authentication Architectural Model*

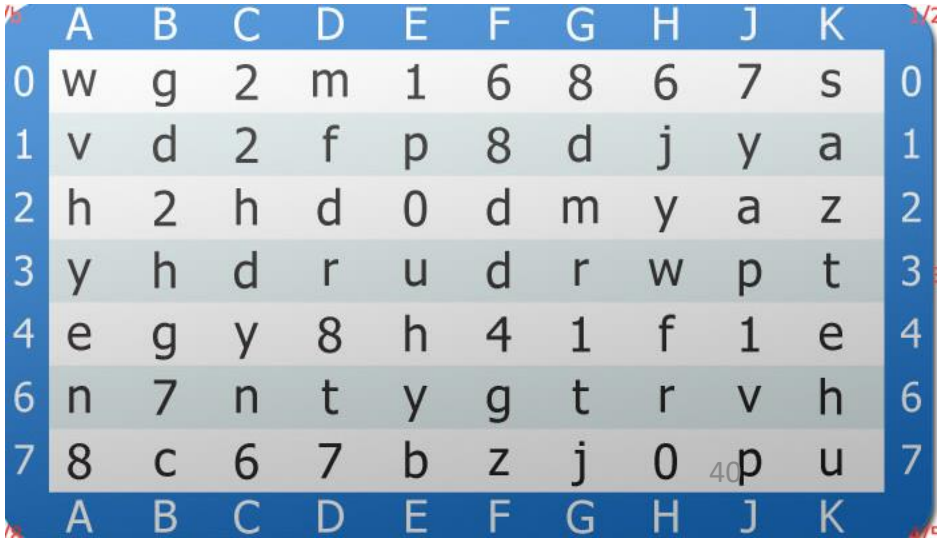
Authenticator Types for e-authentication

1. **Memorized Secrets** – something you know
   - A secret shared between Subscriber and CSP
   - Typically character strings (e.g. passwords, passphrases,) or numerical strings (PINs)
   - Authenticator presented to the Verifier in an authentication process is the secret itself (e.g. password, passphrase, or PIN itself)

Authenticator Types for e-authentication

2. Look-up Secret – something you have

- The secret(s) identified by a prompt
- A physical or electronic authenticator that stores a set of secrets shared between the Claimant and the CSP
- Claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the Verifier (the authenticator input)
- E.g. Claimant asked by the Verifier to provide a specific subset of the numeric or character strings printed on a card in table format



	A	B	C	D	E	F	G	H	J	K	
0	w	g	2	m	1	6	8	6	7	s	0
1	v	d	2	f	p	8	d	j	y	a	1
2	h	2	h	d	0	d	m	y	a	z	2
3	y	h	d	r	u	d	r	w	p	t	3
4	e	g	y	8	h	4	1	f	1	e	4
6	n	7	n	t	y	g	t	r	v	h	6
7	8	c	6	7	b	z	j	0	p	u	7
	A	B	C	D	E	F	G	H	J	K	

Authenticator Types for e-authentication

3. Out of Band authenticator

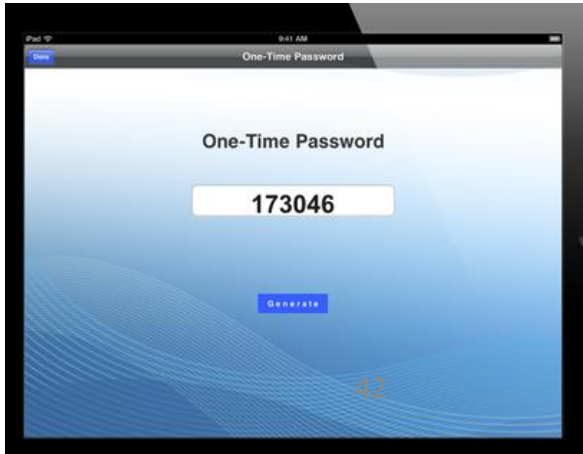
- Physical device uniquely addressable
- Receives a Verifier-selected secret sent to the Claimant's device for one-time use
- Is possessed and controlled by Claimant
  - *Supports private communication over a channel that is separate from the primary channel for e-authentication*
- **Value** provided by the Out of Band authenticator is presented to the Verifier using the primary channel for e-authentication

E.g. Claimant attempts to log into a website and receives a text message on his/her cellphone with a random authenticator to be presented as part of the electronic protocol

Authenticator Types for e-authentication

4. Single-factor (SF) One-Time Password (OTP) – something you have

- **Authentication achieved via** the one-time password
- A hardware device that supports the spontaneous generation of one-time passwords
- This device has an embedded secret that is used as the seed for generation of one-time passwords and does not require activation through a second factor
- Authentication is accomplished by providing an acceptable one-time password and thereby proving possession and control of the device
- E.g. the one-time password device may display 6 numbers at a time



Authenticator Types for e-authentication

5. Single-factor (SF) Cryptographic Device– something you have

- **Authenticator** is a signed message
- Hardware device performs cryptographic operations on input provided to the device
- Device uses embedded symmetric or asymmetric cryptographic keys
- Authentication is accomplished by proving possession of the device
- Device does not require activation through a second factor of authentication
  - *E.g. Transport Layer Security (TLS) uses a "certificate verify" message*
    - *The server verifies the client's identity by verifying the client's digital certificate with the public key*

Authenticator Types for e-authentication

6. **Multi-factor (MF) Cryptographic Software** – something you have (and either something you know or something you are)
    - **Authenticator** is a signed message
    - A cryptographic key is stored on disk or some other "soft" media and requires activation through a second factor of authentication
    - Authentication is accomplished by proving possession and control of the key
    - Device requires activation through a second factor of authentication either something you know or something you are (e.g. fingerprint)
        - *E.g. Transport Layer Security (TLS) uses a "certificate verify" message*
            - *The server verifies the client's identity by verifying the client's digital certificate with the public key*

Authenticator Types for e-authentication

8. **Multi-factor (MF) One-Time Password (OTP) Device** – something you have (and either something you know or something you are)
   - **Authenticator** is the one-time password
     - …based on a hardware device that generates one-time passwords for use in authentication and which requires activation through a second factor of authentication
   - Second factor of authentication may be achieved through an integrated
     - Keypad
     - Biometric reader (e.g. fingerprint)
     - Direct computer interface (e.g. USB port)
   - One-time password is typically displayed on the device and manually input to the Verifier as a password, although direct electronic input from the device to a computer is also allowed

Authenticator Types for e-authentication

9. **Multi-factor (MF) Cryptographic Device** – something you have (and either something you know or something you are)
   - **Authenticator** is some type of signed message
     - Based on a hardware device that contains a protected cryptographic key that requires activation through a second authentication factor
     - Authentication accomplished by proving possession of the device and control of the key
     - May be activated by something you know or something you have

Authenticator Usage

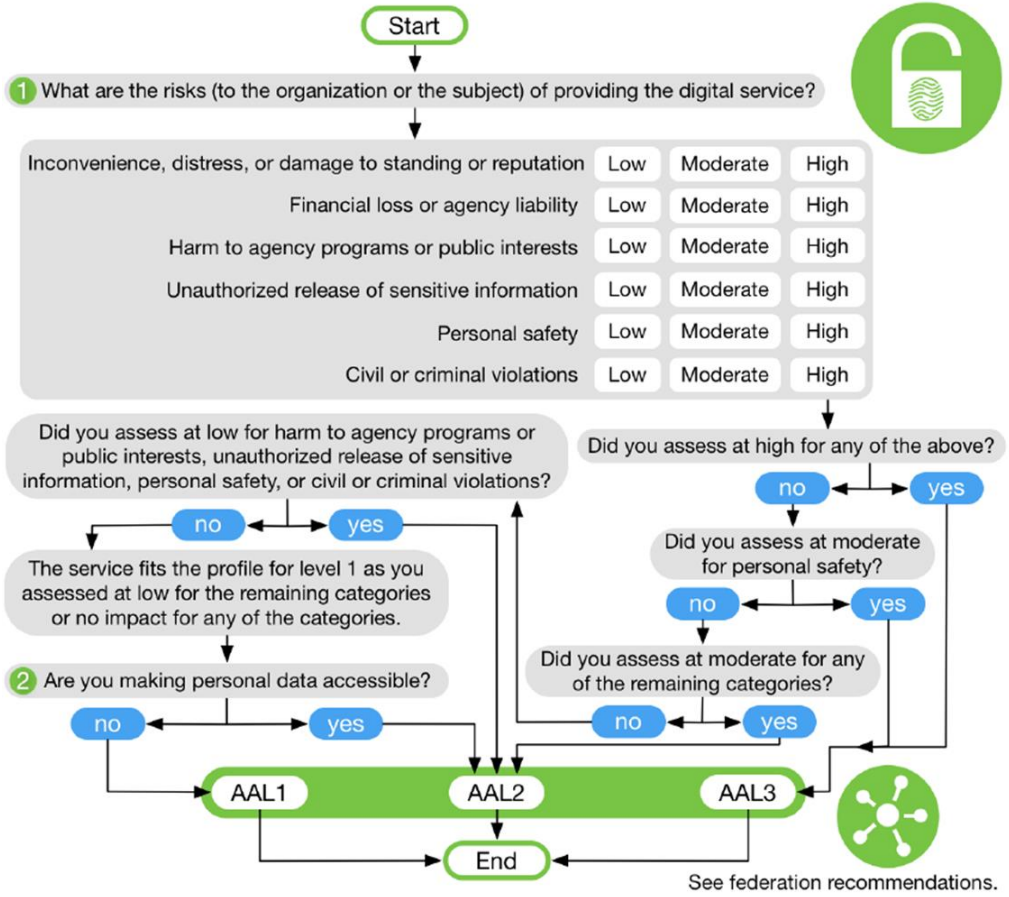
An authentication process may involve a single authenticator, or a combination of two or more authenticators:

- **Single authenticator** – Claimant presents a single authenticator to prove their identity to the Verifier
  - E.g. Claimant attempts to log into a password protected website, the Claimant enters a username and password
  - In this instance, only the password is considered to be an authenticator

- **Multi-authenticator authentication** – Claimant presents values generated by two or more authenticator to prove his/her identity to the Verifier
  - The combination of authenticators is characterized by the combination of factors used by the authenticators (both inherent in the manifestation of the authenticators, and those used to activate the authenticators)
  - E.g. Verifier requires a Claimant to enter a password and use a single-factor cryptographic device is an example of a multi-authenticator authentication
    - The combination is considered multi-factor, since the password is *something you kno*w and the cryptographic device is *something you have*

AAL = Authenticator Assurance Level

AAL1 : = 1 Factor
AAL2 : = 2 Factors
AAL3 : = 2 Factors: Hardware-based authenticator and an authenticator that provides verifier impersonation resistance



Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier-Impersonation Resistance	Not required	Not required	Required
Verifier-Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

A “draft” attempt at summarizing use of Authenticators for Authentication Assurance Levels

Something you...		know	have	have	have	have	have + (know or are)	have	have + (know or are)	have + (know or are)
Something you...		**Memorized Secret**	**Look-up Secret**	**Out of Band Device**	**Single-Factor OTP Device**	**Single-Factor Cryptographic Software**	**Multi-Factor Cryptographic Software**	**Single-Factor Cryptographic Device**	**Multi-Factor OTP Device**	**Multi-Factor Cryptographic Device**
know	**Memorized Secret**	AAL1	AAL2	AAL2	AAL2	AAL2	AAL2	AAL3	AAL3	AAL3
have	**Look-up Secret**		AAL1	AAL1	AAL1	AAL1	AAL2	AAL1	AAL3	AAL3
have	**Out of Band Device**			AAL1	AAL1	AAL1	AAL2	AAL1	AAL3	AAL3
have	**Single-Factor OTP Device**				AAL1	AAL1	AAL2	AAL1	AAL3	AAL3
have	**Single-Factor Cryptographic Software**					AAL1	AAL2	AAL1	AAL3	AAL3
have + (know or are)	**Multi-Factor Cryptographic Software**							AAL2	AAL3	AAL3
have	**Single-Factor Cryptographic Device**								AAL3	AAL3
have + (know or are)	**Multi-Factor OTP Device**									AAL3
have + (know or are)	**Multi-Factor Cryptographic Device**									AAL3

Authenticator Threats

Something you have…

- May be lost, damaged, stolen from the owner or cloned by the Attacker
  - *E.g. Attacker who gains access to the owner's computer might copy a software authenticator*
  - *E.g. A hardware authenticator might be stolen, tampered with, or duplicated*

Authenticator Threats

Something you know…

- May be disclosed to an Attacker
- Attacker might guess a password or PIN
- Where the authenticator is a shared secret, the Attacker could gain access to the CSP or Verifier and obtain the secret value
- An attacker may observe the entry of a PIN or passcode, find a written record or journal entry of a PIN or passcode, or may install malicious software (e.g. a keyboard logger) to capture the secret
- An attacker may determine the secret through off-line attacks on network traffic from an authentication attempt
- An attacker may be able to gain information about a Subscriber's Pre-registered Knowledge researching the subscriber or through other social engineering techniques (e.g. the subscriber might refer to his/her pet in a conversation or blog)

Authenticator Threats

- *Something you are (biometrics)…*
  - May be replicated

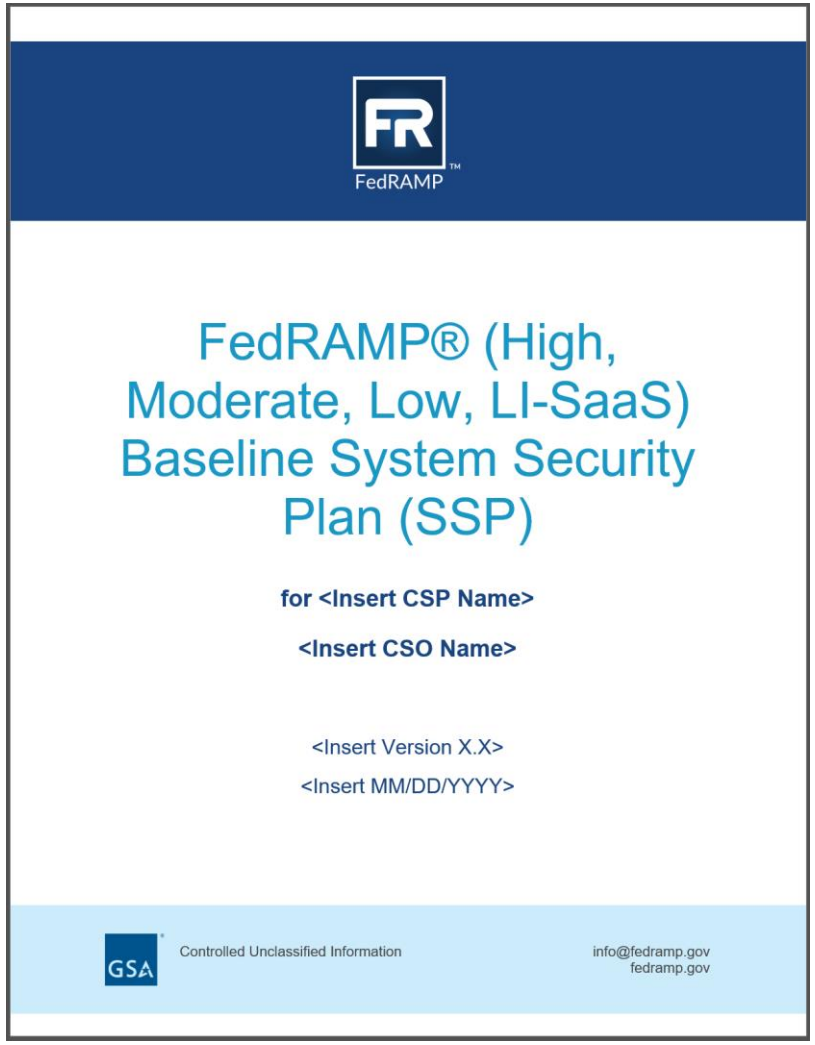
    An Attacker may obtain a copy of the authenticator owner's fingerprint and construct a replica – assuming that the biometric system(s) employed to not block such attacks by employing robust liveness detection techniques

Biometrics – when employed as a single factor of authentication by themselves may not be an acceptable technique for e-authentication

Scanning fingerprint from display


Bkav
Bkav

Digital Identity Determination for your SSP



FedRAMP

FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)

for <Insert CSP Name>

<Insert CSO Name>

<Insert Version X.X>

<Insert MM/DD/YYYY>

GSA Controlled Unclassified Information

info@fedramp.gov
fedramp.gov

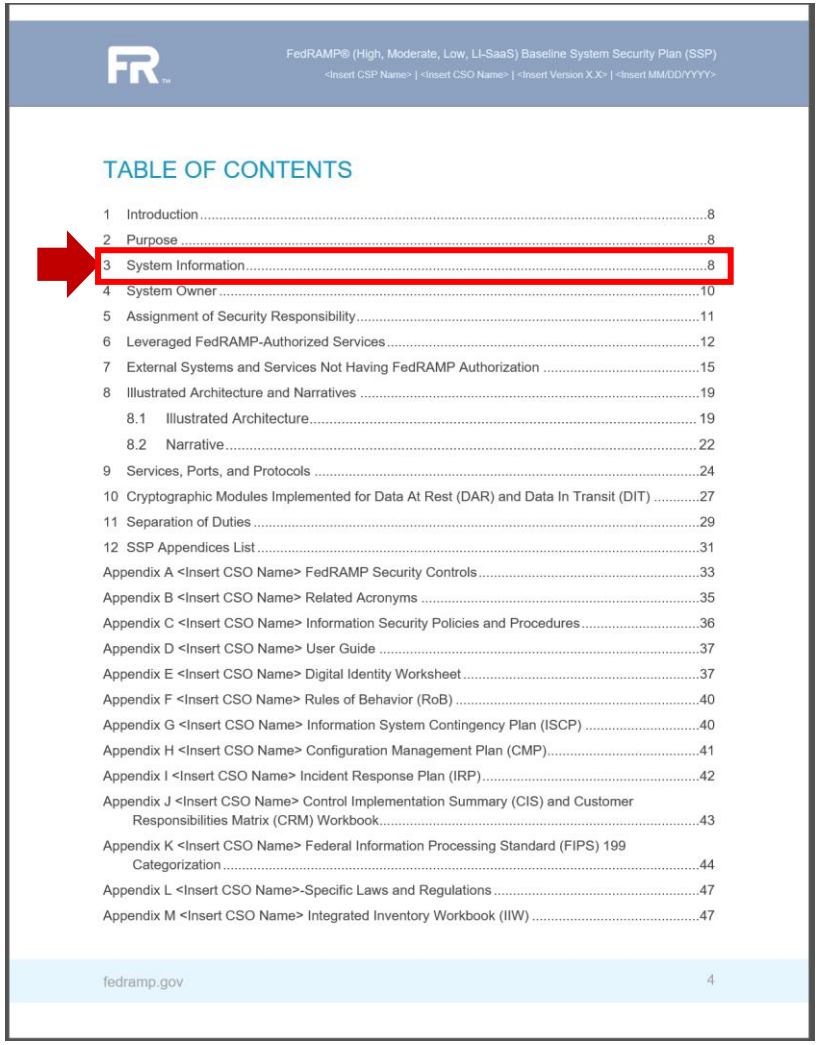
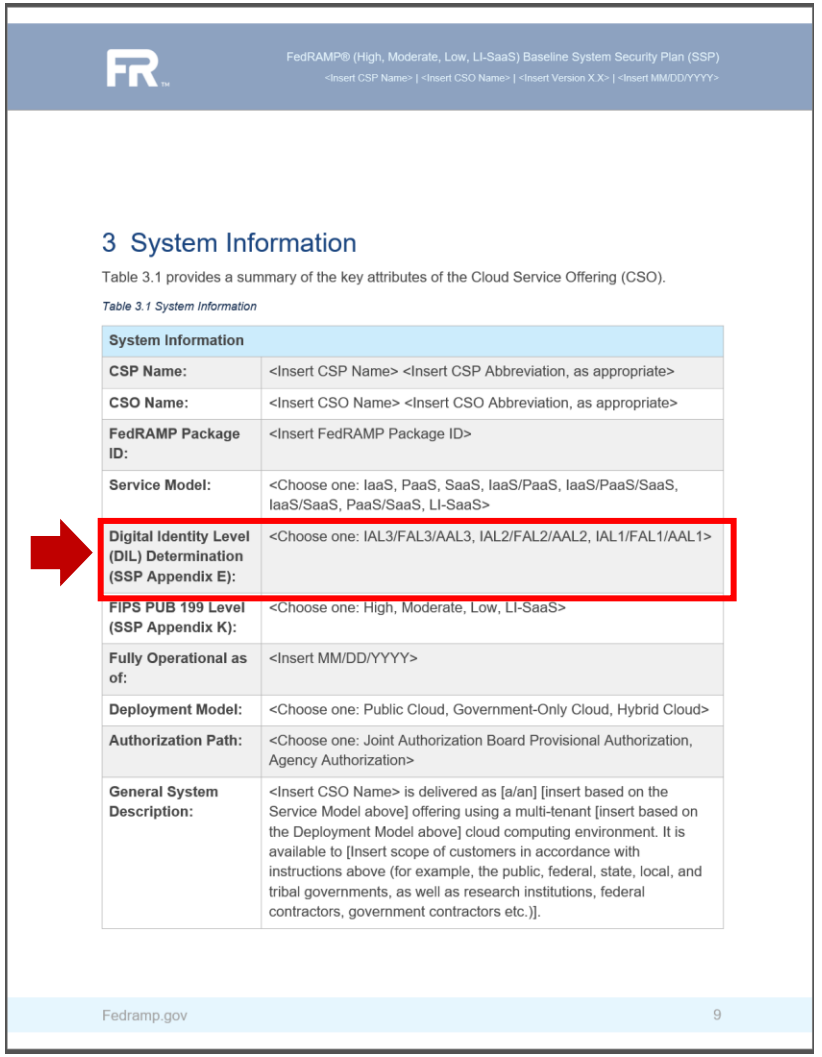


TABLE OF CONTENTS



3 System Information

Table 3.1 provides a summary of the key attributes of the Cloud Service Offering (CSO).

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
General System Description:	<Insert CSO Name> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

Digital Identity Determination for your SSP

Appendix E <Insert CSO Name> Digital Identity Worksheet

Mapping FedRAMP Levels to NIST SP 800-63 Levels

Digital identity is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on the identity proofing process, the authenticator management process, and the assertion protocol used in a federated environment to communicate authentication and attribute information, if applicable.

Table E.1, below, "Mapping FedRAMP Levels to NIST SP 800-63 Levels", maps the FedRAMP impact levels (Low/LI-SaaS, Moderate, and High) to NIST SP 800-63 Digital Identity Guidelines levels:

- Identity Assurance Level (IAL) - Refers to the identity proofing process
- Authenticator Assurance Level (AAL) - Refers to the authentication process
- Federation Assurance Level (FAL) - Refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable), to a relying party (RP)

Table E.1 Mapping FedRAMP Levels to NIST SP 800-63 Levels

FedRAMP Impact Level	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person or supervised remote identity proofing	AAL3: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography; authenticator must be hardware-based	FAL3: The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it. For very high value or very high-risk situations, the subscriber (user) must provide proof of possession of a secure, cryptographic key, and a HW based device to provide verifier impersonation resistance. The device may fulfill both requirements.
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low and FedRAMP LI-SaaS	IAL1: Self-asserted	AAL1: Single-factor or multi-factor; verifiers use FIPS 140-validated cryptography	FAL1: Assertion is digitally signed by the identity provider

Digital Identity Level Selection

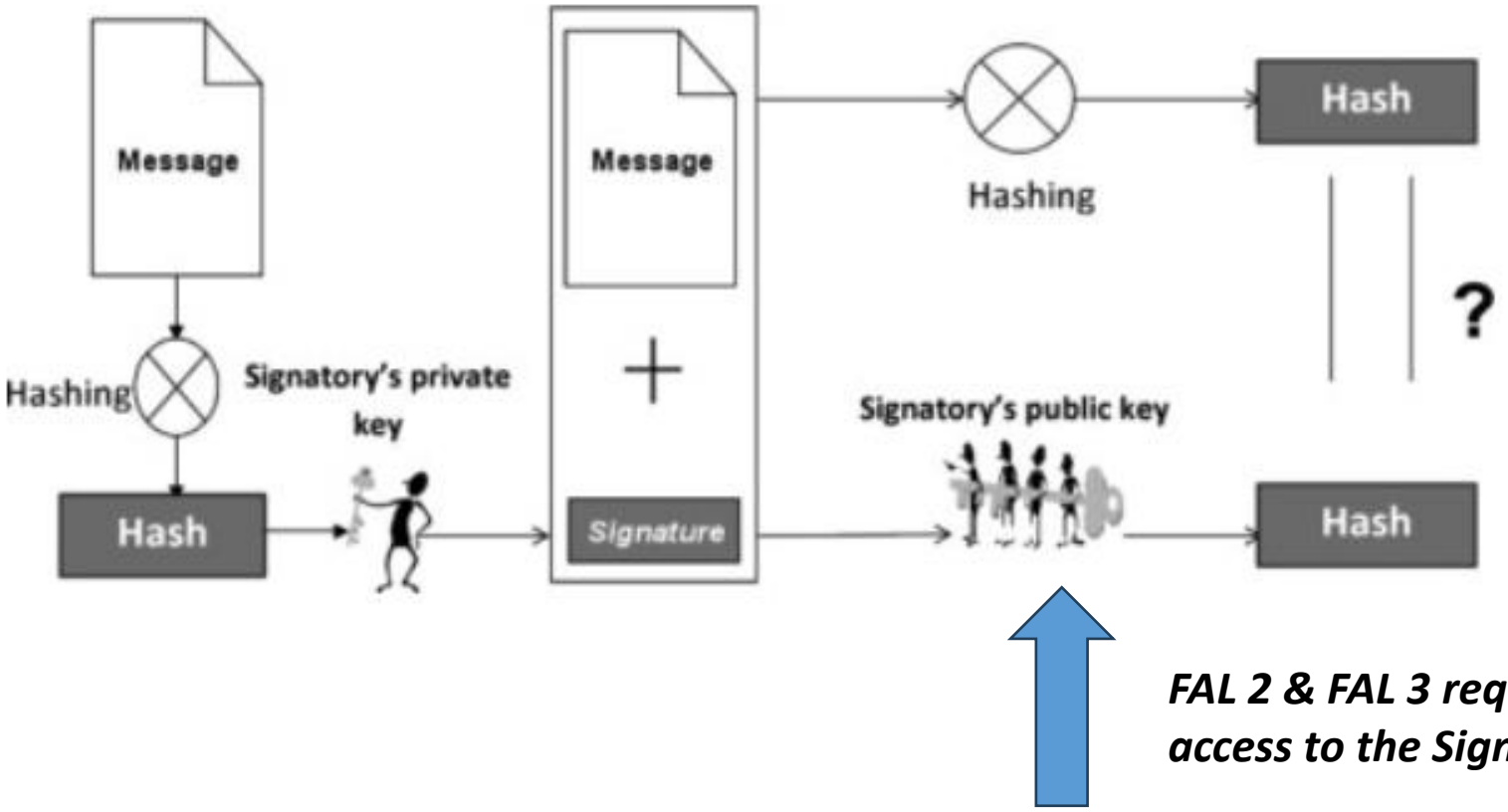
The <Insert CSP Name> has identified that they support the digital identity level that has been selected for the <Insert CSO Name>. The selected digital identity level indicated is supported for federal agency consumers of the CSO. Implementation details of the digital identity mechanisms are provided in Appendix A under control IA-2.

Table E.2 Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Low/LI-SaaS	☐
Level 2: AAL2, IAL2, FAL2	Moderate	☐
Level 3: AAL3, IAL3, FAL3	High	☐

Digital Signature for FedRAMP FAL1-3

The act of signing means encrypting the message's hash value with the private key



FAL 2 & FAL 3 requires control of who gains access to the Signatory's public Key

Agenda

- ✓New schedule for today's classes and mid-term exam
- ✓Access Control
- ✓Identification and Authentication
  - ✓Digital Identity Guidelines
- Centralized Remote Access Control Technologies

Centralized Remote Access Control Technologies

Use what is referred to as “AAA Protocol” (“*triple A*”)

- Authentication, Authorization, and Auditing (or Accounting)
  - Early traditional AAA Protocols include (*more on these and their improvements later*…):
    - Password Authentication Protocol (PAP)
    - Challenge Handshake Authentication Protocol (CHAP)
    - Extensible Authentication Protocol (EAP)

RADIUS – Remote Authentication Dial-In User Service (RADIUS)

TACACS – Terminal Access Controller Access Control System (TACACS)

TACACS+

Diameter – *Is <u>not</u> an acronym*

PAP – Password Authentication Protocol

- All network operating systems support PAP
- PAP authentication requires the calling device to enter the username and password
  - If the credentials match with the local database of the called device or in the remote AAA database then it is allowed to access otherwise denied
  - PAP is considered “less secure” as the password is sent in clear text and is performed only at the initial link establishment
  - It uses a two-way Handshake Protocol
  - It is non-interactive
  - Supports both one-way authentication (unidirectional) and two-way authentication (bidirectional)

CHAP – Challenge Handshake Authentication Protocol

- It is used at the initial startup of the link
- It also performs periodic checkups to check if the router is still communicating with the same host.
- CHAP (3-way authentication) is more secure than PAP (2-way authentication)
  - It uses 3-way handshaking protocol (not like TCP)
    - 1st the authenticator sends a challenge packet to the peer
    - 2nd the peer responds with a value using its one-way hash (MD5) function
    - 3rd the authenticator then matches the received value with its own calculated hash (MD5) value
      - If the values match then the authentication is acknowledged otherwise, the connection will be terminated

EAP – Extensible Authentication Protocol

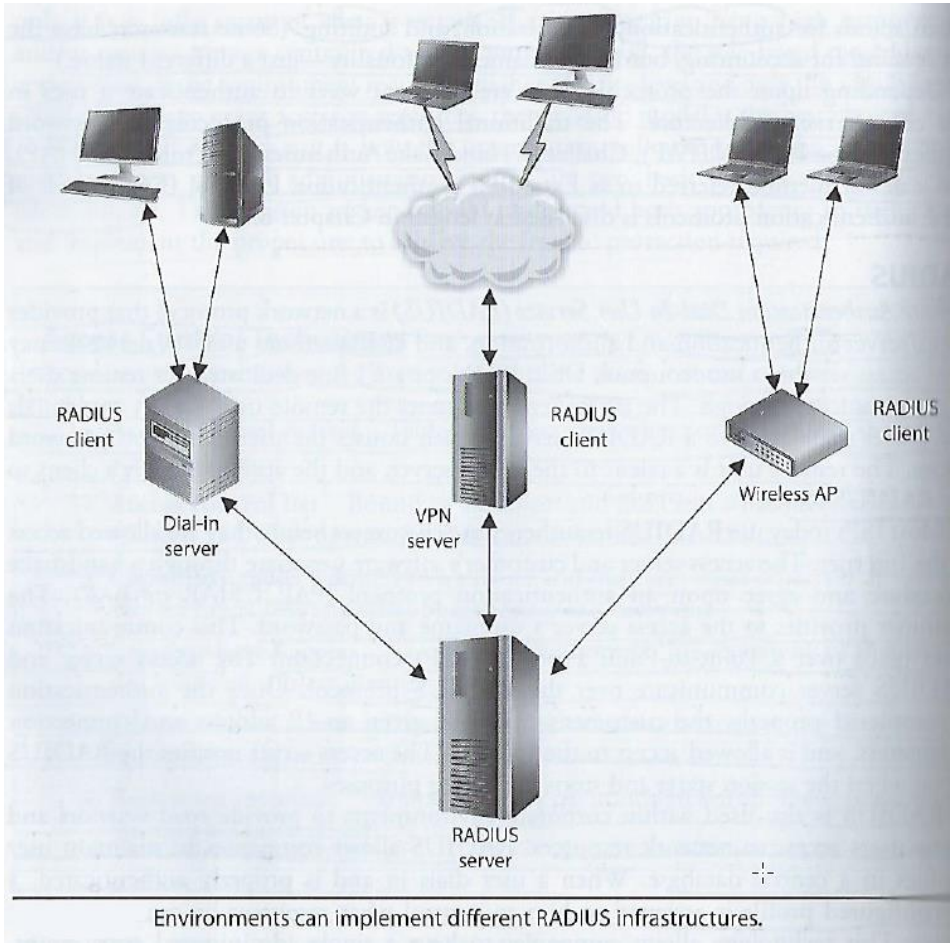
EAP is not an authentication method like PAP or CHAP, but rather a framework on the access client and authentication server that allows networking vendors to develop and easily install new authentication methods known as EAP methods

- There are ~40 different EAP methods available, including:
  - Lightweight Extensible Authentication Protocol (LEAP), credentials are not strongly protected and easily compromised
  - EAP Transport Layer Security (EAP-TLS), considered one of the most secure EAP standards available
    - The majority of implementations of EAP-TLS require mutual authentication using client-side X.509 certificates without giving the option to disable the requirement
  - EAP Protected One-Time Password (EAP-POTP), EAP Pre-Shared Key (EAP-PSK), EAP Password (EAP-PWD), EAP Tunneled Transport Layer Security (EAP-TTLS), EAP Internet Key Exchange v. 2 (EAP-IKEv2), Tunnel Extensible Authentication Protocol (TEAP), EAP Subscriber Identity Module (EAP-SIM), EAP Authentication and Key Agreement (EAP-AKA), EAP Encrypted Key Exchange (EAP-EKE), EAP Generic Token Card (EAP-GTC), …

RADIUS - Remote Authentication Dial-In User Service

Network protocol providing:

- Client/server authentication, authorization and audits of remote users
- Single administered entry point, with standardized security and simple way to track usage and network statistics
- Runs in the application layer, and can use either TCP or UDP as transport
- Created by Livingston Enterprises – then published as a set of open protocol standards (RFC 2865 and RFC 2866)
- Today:
  - Most Internet Service Providers (ISPs) use RADIUS to authenticate their customers before they are provided access to the Internet
  - Many corporations use RADIUS to provide remote and home user employees to access their network resources



Environments can implement different RADIUS infrastructures.

Harris, S. and Maymi F. (2016) All in One CISSP Exam Guide, Seventh Edition, McGraw Hill Education

RADIUS - Remote Authentication Dial-In User Service

The access server and user's software negotiate a handshake procedure and agree on an authentication protocol (PAP, CHAP, or EAP)

- User provides username and password to the access server via a Point-to-Point protocol (PPP) connection
- Access server and RADIUS server communicate over the RADIUS protocol

- Once the authentication is properly completed
  - User system is given an IP address and connection parameters, and corporate users are provided a preconfigured profile to control which resources they can access

- User credentials and configurations can be held in LDAP (Lightweight Directory Access Protocol) servers, databases or text files
- Network access servers, the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server

RADIUS - Remote Authentication Dial-In User Service

Uses UDP (connectionless)

- Requires RADIUS to have more code to detect and correct transmission errors (packet corruption, long timeouts, or dropped packets)

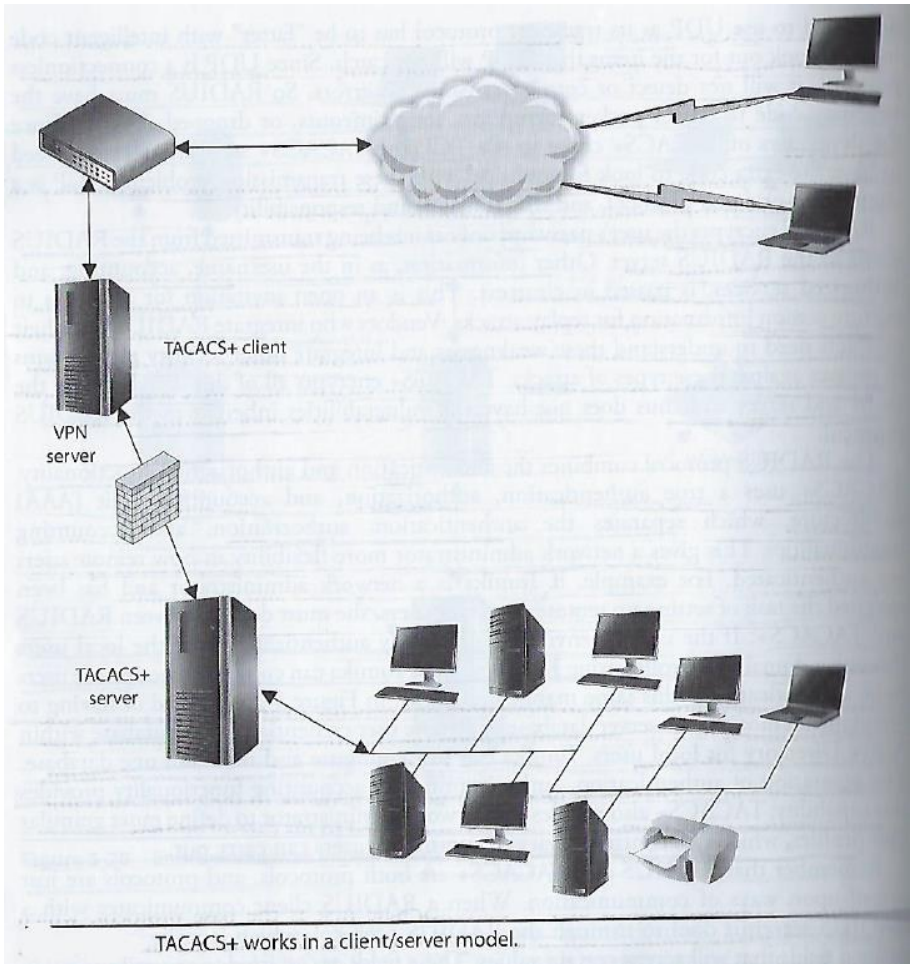
- Encrypts users' password only when transmitted from RADIUS client to RADIUS server
  - Other information is passed in clear text: Username, accounting and authorized services
  - Open invitation for attackers to capture session information for replay attacks
  - Vendors who integrated RADIUS into their products must understand the weaknesses and add additional security capabilities into their products

- Combined authentication and authorization functionality limits flexibility…

TACACS – Terminal Access Controller Access Control System

3 generations

1. TACACS
   - Combines authentication and authorization processes
   - Uses fixed passwords for authentication
2. XTACACS (Extended TACACS)
   - Separates authentication, authorization and auditing processes
3. **TACACS+**
   - Is a different protocol than TACACS and XTACACS



TACACS+ works in a client/server model.

Harris, S. and Maymi F. (2016) All in One CISSP Exam Guide, Seventh Edition, McGraw Hill Education

TACACS+

- Has 2-factor authentication
  - Allows users to one-time (dynamic) passwords for more protection
- Similar functionality as RADIUS but uses TCP
  - Does not need extra code to deal with transmission problems like RADIUS which supports UDP
- Encrypts all data between client and server
  - Does not have the vulnerabilities inherent in RADIUS
- Users true authentication, authorization and accounting/audit (AAA) architecture that separates the 3 functions to provide network administrators more flexibility in how remote users are authenticated
  - Can work with alternative authentication servers (e.g. Kerberos is used in the organization for authentication then it can be used by TACACS+, alternatively if Active Directory is used for local users then that can be used)
  - Can define more granular user privledges to control over the specific commands users can carry out
- Is a protocol with more Attribute Value Pairs (AVPs) than RADIUS
  - Enabling network administrators to use them to define ACLs filters, user privileges and more…

RADUS versus TACACS+

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password from the RADIUS client to the server.	Encrypts all traffic between the client and server.
AAA support	Combines authentication and authorization services.	Uses the AAA architecture, separating authentication, authorization, and auditing.
Multiprotocol support	Works over PPP connections.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Responses	Uses single-challenge response when authenticating a user, which is used for all AAA activities.	Uses multiple-challenge response for each of the AAA processes. Each AAA activity must be authenticated.

Specific Differences Between These Two AAA Protocols

TACACS+ is a better choice for corporate networks needing better authentication and control of authorization

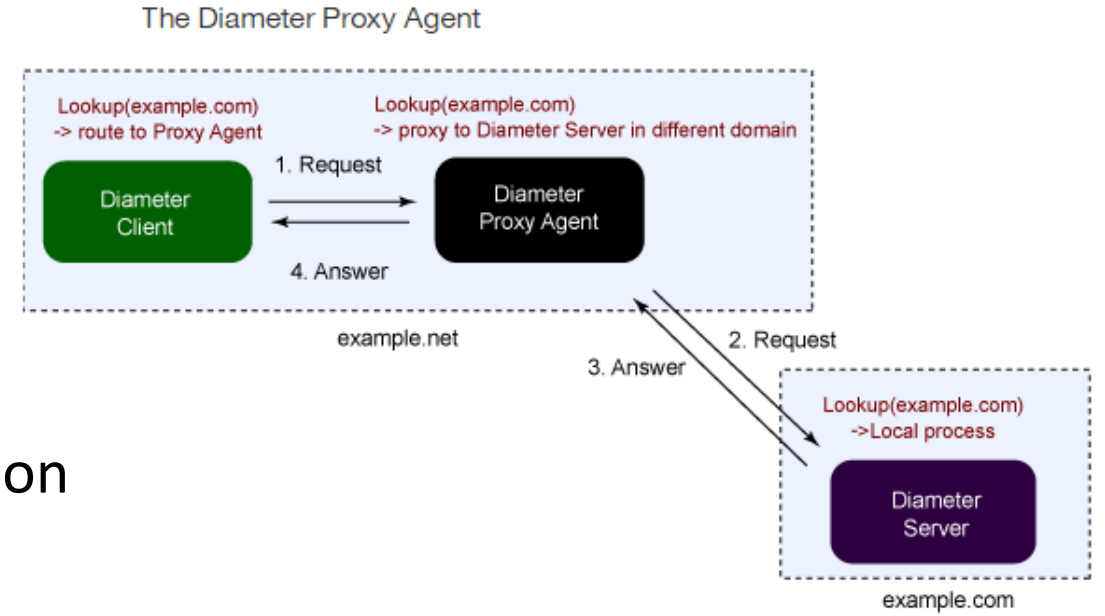
Harris, S. and Maymi F. (2016) All in One CISSP Exam Guide, Seventh Edition, McGraw Hill Education

Diameter – "*twice the radius*"

Enhanced AAA protocol providing similar functionality as RADIUS and TACACS+, but with greater flexibility and capabilities

- Consists of 2 portions:
  1. Base protocol – secure communication among Diameter entities, feature discovery and version negotiation
  2. Extensions – allowing various technologies to use Diameter authentication, authorization and auditing capabilities
     - Supports interoperability with wireless devices, smartphones, Voice over IP (VOIP), Mobile IP (coordinates transfer or traffic between care-of-address and home IP address)
- Peer-based protocol
  - Not Client/Server (which requires client and server to take turns sending data between them)
  - Either end can initiate communication

Diameter – “twice the radius”



- Authentication
  - PAP, CHAP, EAP
  - End-to-end protection of authentication information
  - Replay attack protection
- Authorization
  - Redirects, secure proxies, relays, and brokers
  - State reconciliation
  - Unsolicited disconnect
  - Reauthorization on demand
- Accounting/Auditing
  - Reporting, roaming operations (ROAMOPS) accounting, event monitoring

Diameter Versus RADIUS

	Diameter	RADIUS
Transportation Protocol	Connection-Oriented Protocols (TCP and SCTP)	Connectionless Protocol (UDP)
Security	Hop-to-Hop, End-to-End	Hop-to-Hop
Agent Support	Relay, Proxy, Redirect, Translation	Implicit support, which means the agent behaviors might be implemented in a RADIUS server
Capabilities Negotiation	Negotiate supported applications and security level	Don't support
Peer Discovery	Static configuration and dynamic lookup	Static configuration
Server Initiated Message	Supported. for example, re-authentication message, Session termination	Don't support
Maximum Attribute Data Size	16,777,215 octets	255 octets
Vendor-specific Support	Support both vendor-specific messages and attributes	Support vendor-specific attributes only

Liu, J., Kiang, S., and Lin, H. (2006) “Introduction to Diameter – Get the next generation AAA protocol”, IBM developerWorks

Agenda

- ✓Access Control
- ✓Identification and Authentication
  - ✓Digital Identity Guidelines
- ✓Centralized Remote Access Control Technologies