Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 05: Identity and Access Management (IAM)

Learning Objectives

By the end of this lesson, you will be able to:

- Control physical and logical access to assets to ensure data security and prevent unauthorized access
- Control identification and authentication of people, devices, and services to verify identities and protect organizational resources
- Implement and manage authorization mechanisms to ensure appropriate access levels for users and systems
- Administer the identity and access provisioning lifecycle to maintain secure and compliant access to resources

Introduction to Identity and Access Management

Identity and Access Management (IAM)

It is a framework that controls access to IT resources within an organization.

Key components to ensure proper access and security are:

- Authentication
- Authorization
- Account provisioning
- Account deprovisioning
- Password management
- Role-based access control (RBAC)

Importance of IAM in Information Security

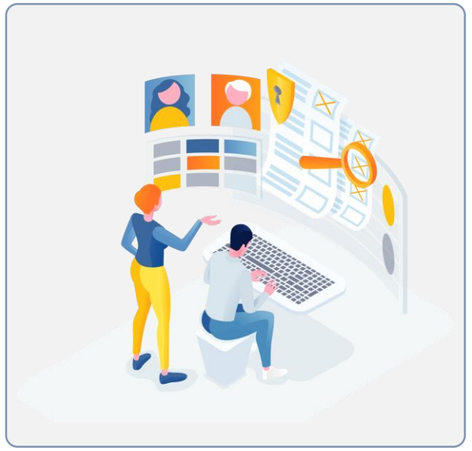
IAM is used to protect networks, applications, and data from attack is of utmost importance.

This is achieved by:

- Auditing current security practices, policies, and processes to suggest improvement actions to be implemented
- Examining and authenticating security through penetration testing and vulnerability assessments

IAM Components

Access is the transfer of data between subjects and objects.



Subject is an active component that needs access to an object or the data within it.

Object is a passive component that contains data or information.

Access control is the security feature that controls user or system interaction with other systems and resources.

Controlling Access to Assets

Information	Access control must be implemented to prevent unauthorized access to the information that could lead to loss of data confidentiality, integrity, and availability.
Systems	Access to IT systems must be regulated to restrict who or what can view or use resources in a computing environment.
Devices	Access to computing devices must be restricted and with the rise of BYOD policies, organizations must implement mobile device management (MDM).
Facilities	Facilities must be protected to limit physical access to only authorized personnel and access to restricted areas must be controlled, tracked, and audited.
Applications	Application access controls must be used to manage user authentication and implement rules that determine user access to applications and data.

Identity and Access Management Policy

An effective access control program in an organization begins with establishing identity and access management policies. These policies include:

Specifying access: Proper identification and authentication for users and programs

Preventing inconsistencies: Consistency in provisioning, administration, and access control management

Granting privileges: Guidelines for accessing various resources

Improving governance: Process for governance

Identity Management

It involves the use of products to identify, authenticate, and authorize users through automated means. Its goals include:

Increasing security and productivity

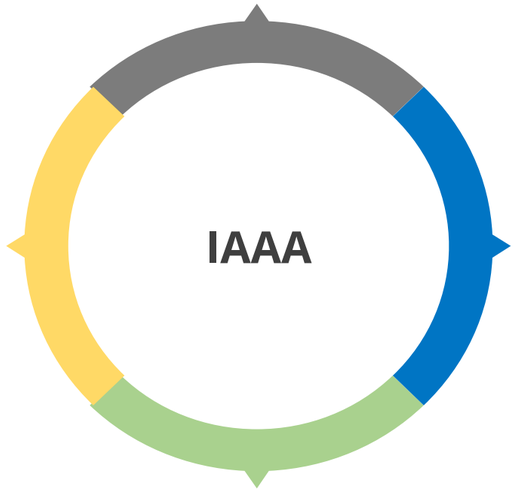
Reducing cost, downtime, and repetitive tasks

IAM Processes

This system consists of four main processes:

Identification
Associating a valid subject with a computer or network account

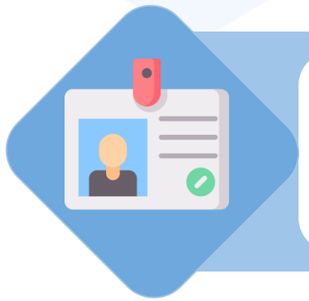
Accounting
Auditing the use of the account



Authentication
Providing credentials to operate the account

Authorization
Assigning rights, permissions, or privileges to the account

Identification



It is the process of an individual claiming or professing an identity.

A subject must submit an identity to the system to begin authentication, authorization, and accountability procedures.

Identification Methods

Digital identification methods are used to authorize applications to access sensitive resources.

Common types include:

- Username
- User ID
- Account number
- Personal identification number (PIN)
- Identification badge
- MAC address
- IP address
- Email address
- Radio frequency identification (RFID)

Guidelines for User Identification

Three important security characteristics of identity are:

Uniqueness

User identification must be unique.

Non-descriptiveness

The user's role or job function should not be exposed by the identity (ID).

Secure issuance

The ID issuing process must be well-documented and secure.

Authentication

It involves comparing one or more criteria to a database of legitimate identities, such as user accounts, to validate the subject's identity.

Example

Users identify themselves with a username and authenticate by providing a password.

Authorization

It is the process of granting access to an object after the subject has been properly identified and authenticated.

Example

CRUD (create, read, update, and delete) operations

Accounting

It refers to a system's ability to associate users and processes with their actions.

Example

The audit log records user activities like login attempts, resource access, and system configuration changes, helping administrators investigate security incidents.

Multi-Factor Authentication (MFA)

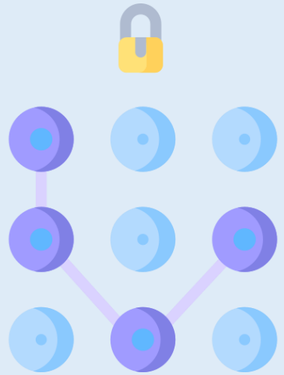
Multi-Factor Authentication (MFA)

It is a type of authentication that necessitates the use of more than one authentication factor to be successful.

Multi-Factor Authentication (MFA)

Based on the type of authentication, MFA can be categorized into:

Something you know

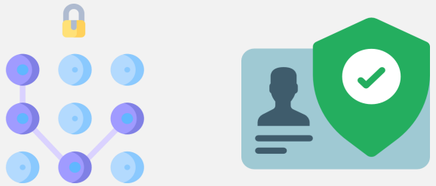


Something you have

Something you are

MFA: Types

Two-factor authentication



Uses a combination of any two of three authentication factors available

Example

To withdraw money, an ATM card (something possessed) and a PIN (something known) are required.

Three-factor authentication

Uses all three authentication factors

Example

To access online banking, a password (something known), a security token (something possessed), and a fingerprint scan (something inherent) are required.

Multi-Factor Authentication (MFA)

Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)

- Known as **authentication by knowledge**
- Something that only the user knows
- Least expensive method to implement

Example

Password, PIN, or answers to challenge questions

Multi-Factor Authentication (MFA)

Something you know
(Type 1)

Something you have
(Type 2)

Something you are
(Type 3)

- Known as **authentication by ownership**
- Some physical objects in the possession of the user

Example

Token or smart card

Multi-Factor Authentication (MFA)

Something you know
(Type 1)

Something you have
(Type 2)

Something you are
(Type 3)

- Known as **authentication by characteristics**
- Some physical characteristics of a user
- Most expensive and secure method

Example

Biometrics or a fingerprint

Quick Check

You are working in an organization that requires logging in with a username, PIN, password, and retina scan. How many different types of authentication factors are you using?

A. One

B. Two

C. Three

D. Four

Type 1 Authentication: Password

Password

It is a secret data usually used to confirm a user's identity.

Problems with passwords

- Insecure
- Easily broken
- Subject to repudiation

Common password attacks

- Dictionary (Crack, John the Ripper)
- Brute force, L0phtcrack)
- Hybrid (Dictionary and Brute-force)
- Trojan horse login program (Password sending trojans)
- Social engineering

The combination of username and password is the most common identification and authentication scheme.

Password Types

Passphrase

It is longer than a password and is in the form of a sequence of characters.

- I will pass the CISSP exam.
- Manchester United is my favorite team.
- A quick brown fox jumps over a lazy dog.

Cognitive passwords

It determines an individual's identity based on opinion or fact-based information.

- What is the name of the high school you attended?
- How many family members do you have?
- What is your mother's maiden name?

One-time password (OTP)

It is a dynamic password valid for only one login session or transaction.

- An OTP that a bank sends to a customer via SMS

Password Management

It involves creating, storing, and using secure passwords to protect online accounts and prevent unauthorized access to personal and financial data.

A process governing user passwords should:

- Set password length and time limits
- Create policies for password changes and resets
- Use previous login dates in banners
- Limit unsuccessful logins
- Limit the concurrent connections
- Enable auditing

Password Management

Self service password reset

Any process or technology that enables users to authenticate with an alternate factor and resolve password issues or lockouts independently, without contacting the helpdesk

Assisted password reset

Any process or technology that allows users to reset their password with assistance from the help desk if they have forgotten it or triggered a lockout

Password synchronization

A process, often supported by password management software, that enables a user to maintain a single password across multiple IT systems

Password-Based Attacks

Electronic monitoring (Replay attack)
Attacker listens to network traffic to capture authentication information and replays it to bypass security measures

Accessing password file
Attacker targets the authentication server to capture the password file, which provides access to passwords for many users

Brute-force attack
Attacker uses automated tools to cycle through all possible combinations in an attempt to crack the password dump

Dictionary attack
Attacker compares thousands of dictionary words to a user's password to find a successful match

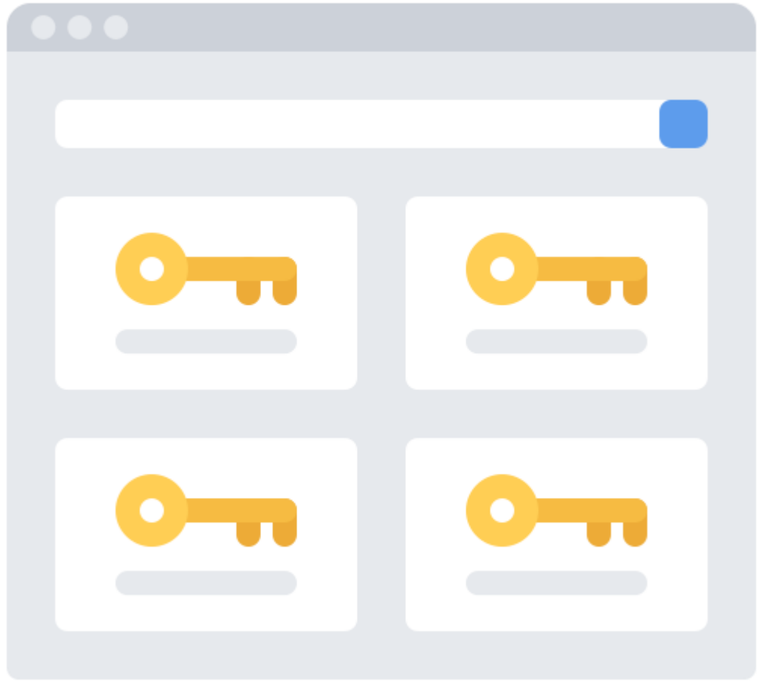
Social engineering
Attacker convinces an individual to share their authentication information through deceptive means

Using rainbow table
Attacker utilizes a table containing hash values for all possible passwords to quickly find the original password from its hash

Password Manager

It is a software application that securely stores and manages users' login credentials for various online accounts and applications.

- Encrypts passwords and other sensitive data (such as credit card numbers or notes) using robust encryption algorithms
- Generates complex, random passwords that are nearly impossible to guess or crack
- Offers cross-device syncing, allowing access to passwords from any device, whether it is a computer, phone, or tablet



Quick Check

Your organization is updating its password policy to enhance security against brute-force attacks. Which password requirement will be most effective in preventing such attacks?

A. Change the maximum password age from 1 year to 180 days

B. Increase the minimum password length from 8 characters to 16 characters

C. Enhance password complexity by requiring at least three-character classes (uppercase, lowercase, numbers, and symbols)

D. Maintain a password history of at least four previous passwords to prevent reuse

Type 2 Authentication: Tokens

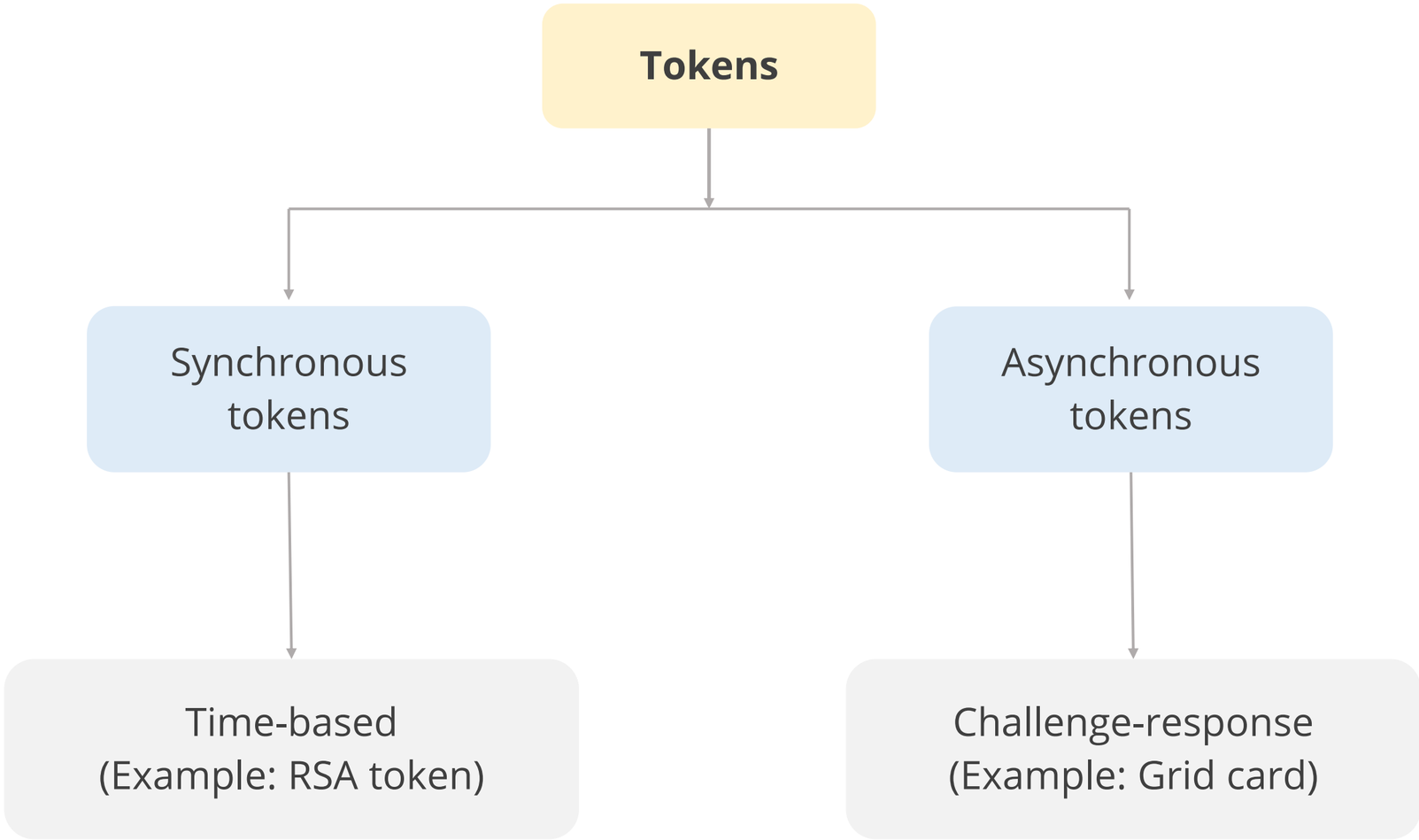
Tokens

A token is a security device that proves a user's identity and facilitates authentication to a system or application.

Attackers can compromise security by gaining control of the token and impersonating the owner, potentially compromising the authentication protocol.

Tokens can be software-based or hardware-based and must be secured from cloning, damage, loss, or theft.

Types of Token



Time-Based One-Time Password (TOTP)

It uses a cryptographic hash function to combine a secret key and a timestamp, creating an encrypted string for multi-factor authentication.

TOTP: Working

1. A secret key is agreed upon and shared between the user and the server.
2. The internal clock between the user's device and the server must be synchronized.
3. The Unix time (seconds since January 1, 1970, 00:00 UTC) is used to generate and validate codes.

TOTP: Working

4. The number of seconds is rounded to 30 seconds by default.

5. The algorithm generates a hash value from the rounded number and the pre-shared secret key.

6. The passcode from the user's device must match the server's passcode associated with the user's device.

Challenge-Response: Token Device

Tokens are generated using a challenge-response scheme to authenticate a user.

1. The challenge number is displayed on the workstation.

2. The user enters the challenge number and PIN permanently associated with the pad.

3. The response is read.

4. The user enters response from pad to the workstation.

5. The authentication server verifies the response.

Example: Working of a grid card

Smart Card

It is a plastic card embedded with a microprocessor or memory chip, offering enhanced security compared to traditional magnetic stripe cards.

Smart Card Attacks

Fault generation attacks

- They introduce computational errors into the cards to uncover the encryption keys used and stored within them.
- The attacker analyzes the encryption process with induced error against the correct results to reverse engineer the encryption process, revealing the key.
- Some methods include, changing the voltage, clock rate, and temperature fluctuation.

Side channel attacks

- They uncover sensitive information without compromising any type of flaw.
- They are primarily used for data collection.
- **Differential power analysis:** Side channel attacks examine the power emissions during processing.
- **Electromagnetic analysis:** They examine the frequencies emitted.
- **Timing:** They estimate how long a specific process takes to complete.

Smart Card Attacks

Software attacks

- It is considered a non-invasive attack.
- It involves inputting instructions into the card to extract information from the card (primarily account information).
- It can be employed in point-of-sale machines used to swipe money.

Microprobing

- It is considered a more intrusive attack.
- It involves using needles and ultrasonic vibrations to remove the protective covering over the circuits.
- Once removed, data can be extracted by directly tapping into the ROM chips.

Quick Check

Bob (M) uses a security token device that changes its code every minute. What type of token device is he using?

A. Synchronous

B. Asynchronous

C. Asymmetric

D. Symmetric

Type 3 Authentication: Biometric

Biometrics

It verifies a person by analyzing the individual's unique physiological or behavioral characteristics, making it one of the most effective and accurate methods of verifying identification.

It belongs to the **something you are** category.

Biometric Authentication

Several types of patterns can be used for biometric identification, which are categorized as follows:

Physical

- Fingerprints
- Iris and facial recognition

Behavioral

- Voice recognition
- Typing pattern matching

Biometric Authentication

The first step in setting up biometric authentication is enrollment, where the selected biometric information is scanned.

The steps involved in the scanning process are:

1

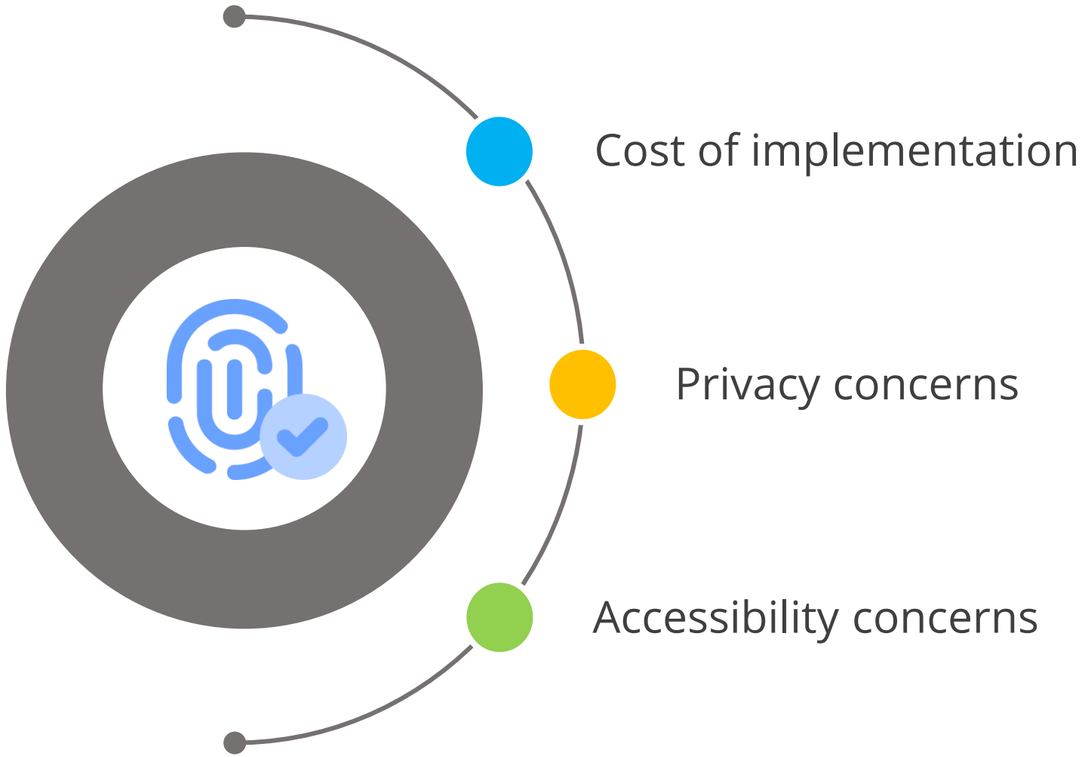
Obtaining biometric samples from the target using the sensor module

2

Recording features that uniquely identify the target in the sample using the feature extraction module

Biometric Authentication

The factors to be considered when implementing biometric authentication are:



Biometrics: Characteristics

Acceptance

Refers to user acceptance of the biometric system, which depends on the privacy intrusiveness and psychological or physical discomfort

Throughput rate (Biometric system response time)

Refers to the time taken to process an authentication request

Enrollment time

Refers to the time taken by the biometric system to register and create an account for the first time

Biometrics: Types

The following are some common types of biometrics:

Keyboard pattern recognition

Facial scan

Retina scan

Iris scan

Voice pattern recognition

Fingerprint

Signature scan

Palm scan

Errors in Access Control

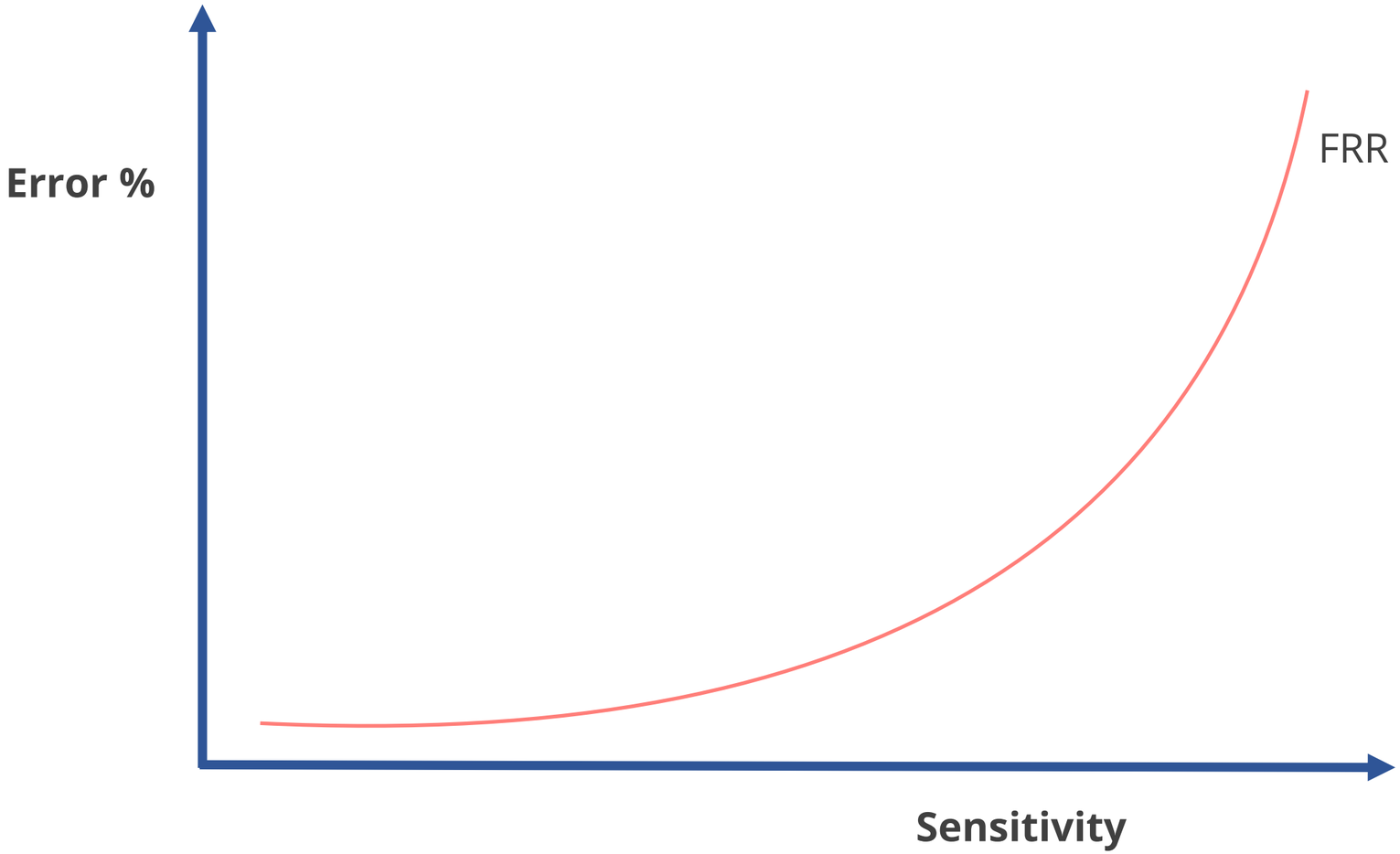
It is crucial to assess the effectiveness of biometric systems and ensure that the system correctly authorizes or rejects users.

Some of the metrics used are:

- False rejection rate (FRR)
- False acceptance rate (FAR)
- Crossover error rate (CER)

Errors in Access Control

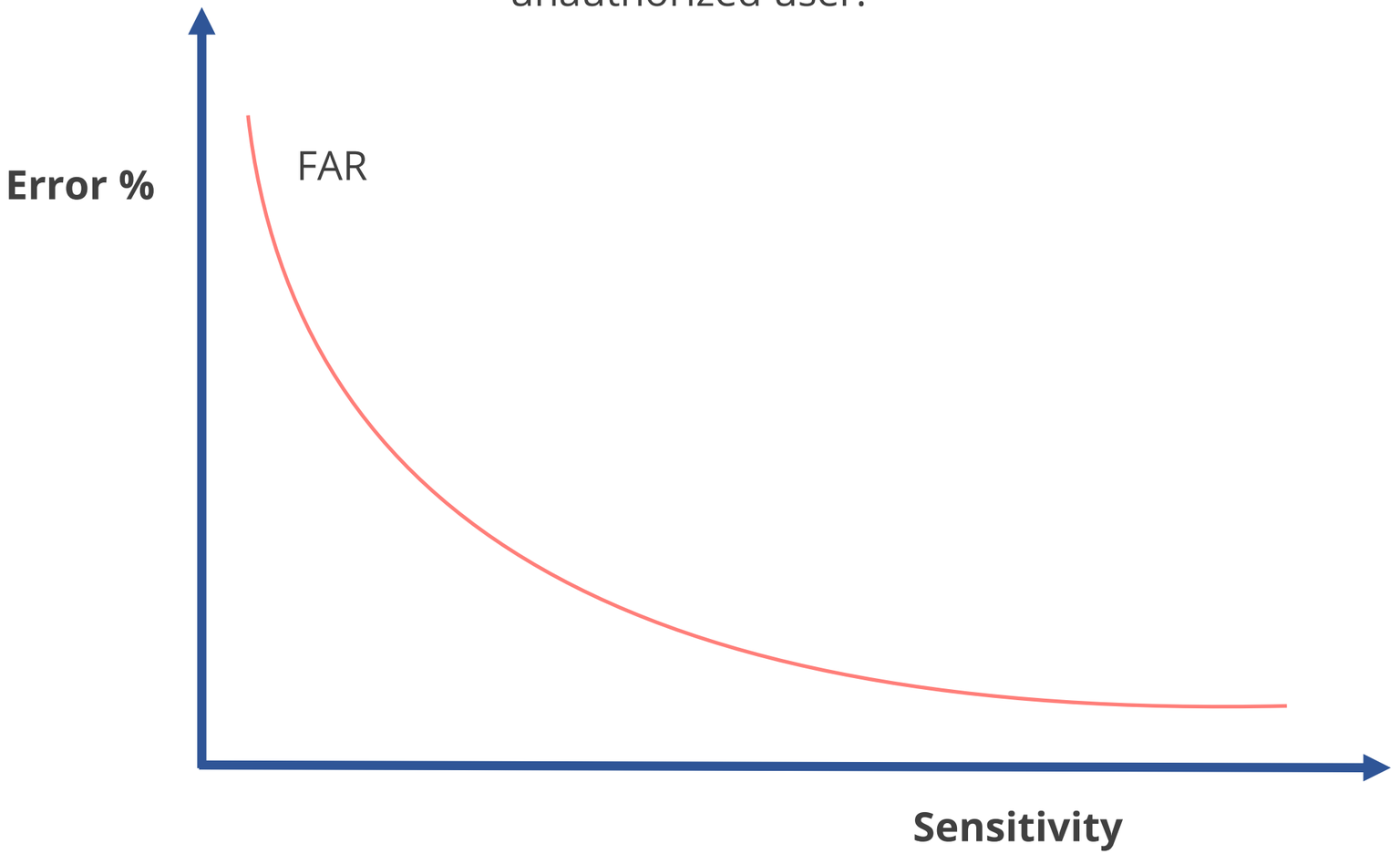
False rejection rate (FRR) occurs when the authentication system falsely rejects a legitimate user.



This is also called false negative or **Type I** error.

Errors in Access Control

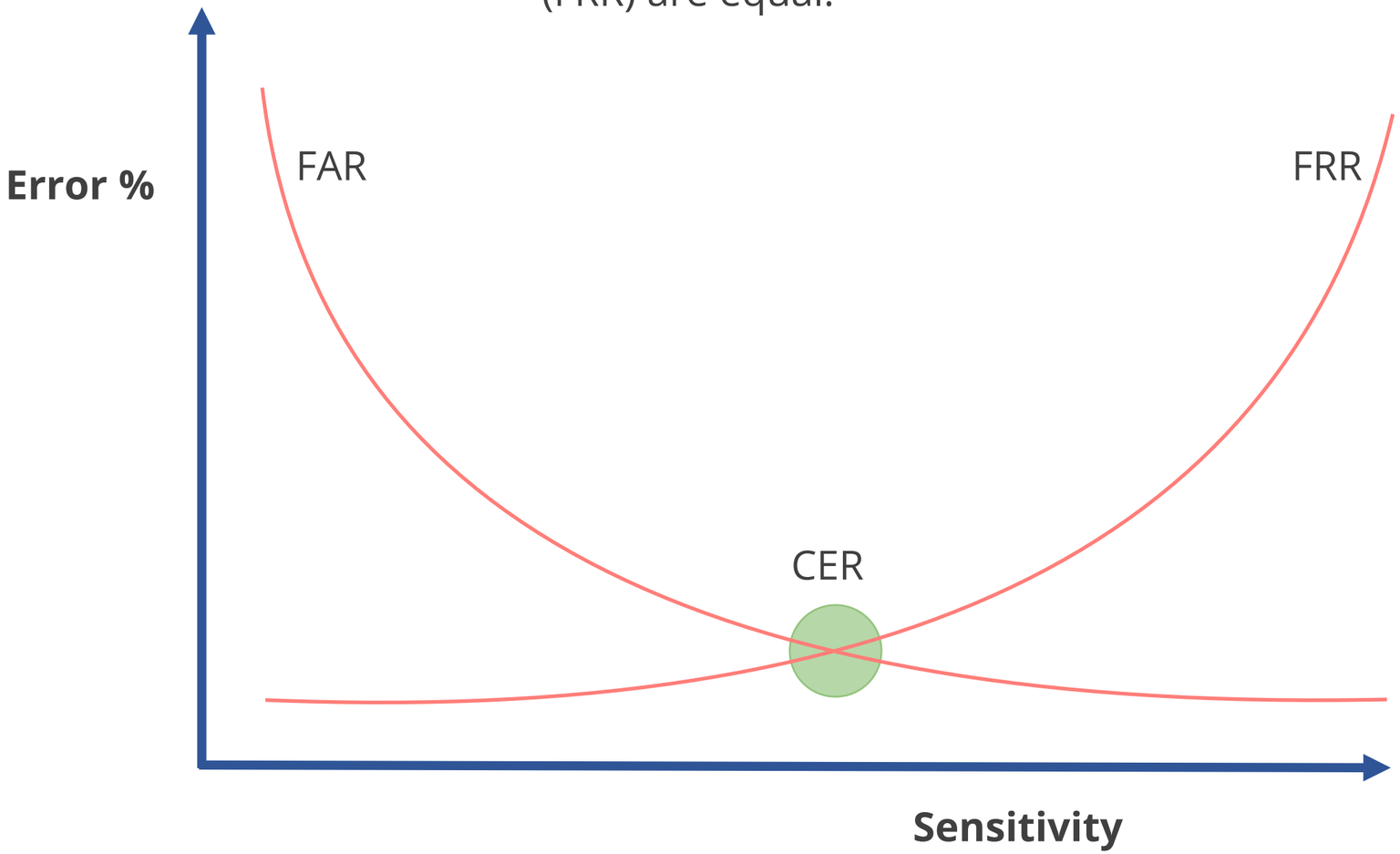
False acceptance rate (FAR) occurs when the authentication system falsely accepts an unauthorized user.



This is also called false positive or **Type II error**.

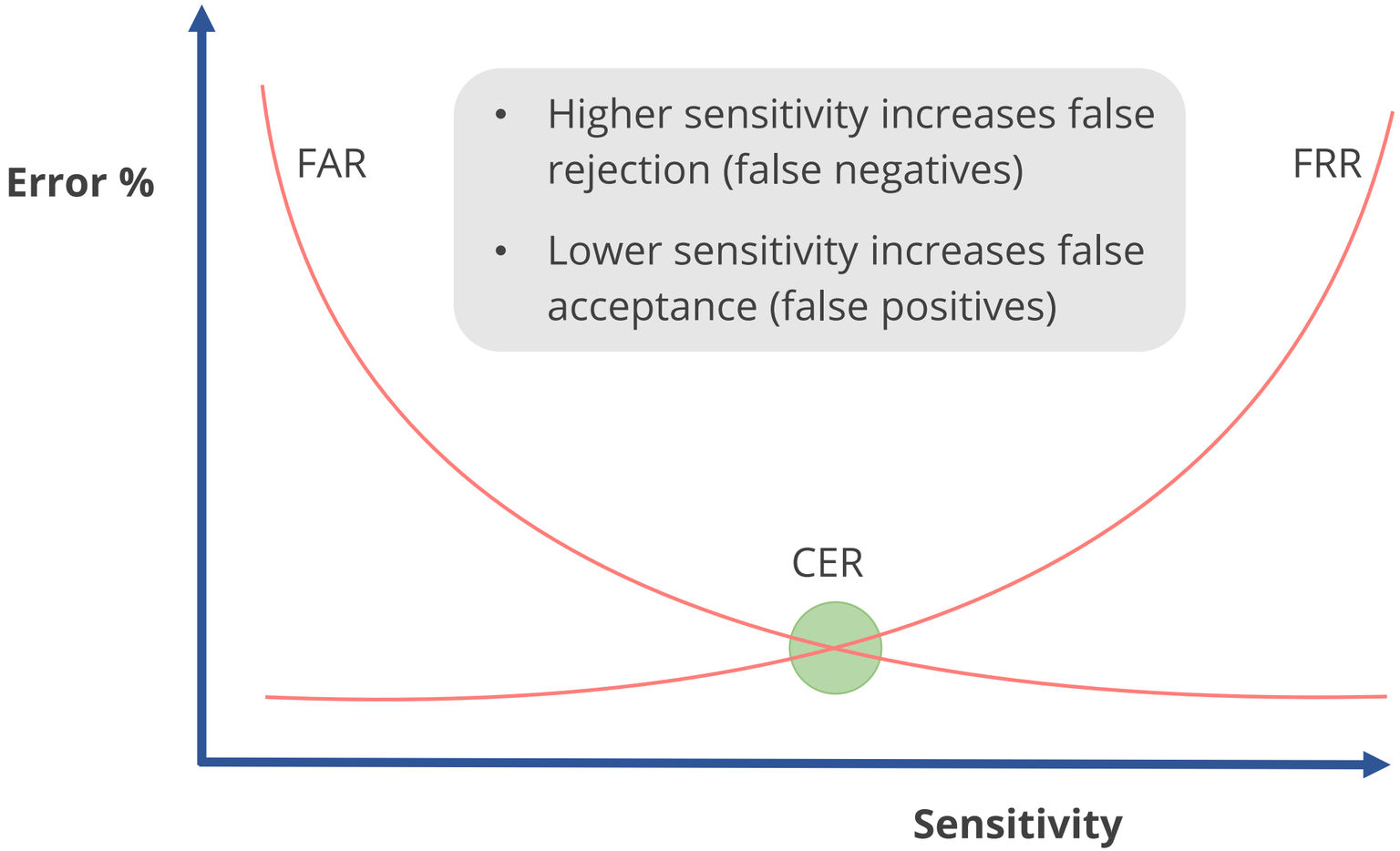
Errors in Access Control

Crossover error rate (CER) is the point where the false acceptance rate (FAR) and the false rejection rate (FRR) are equal.



The lowest CER value indicates the most accurate system.

Errors in Access Control



- Higher sensitivity increases false rejection (false negatives)
- Lower sensitivity increases false acceptance (false positives)

Biometric and Behavioral Technologies

Certain biometric and behavioral technologies can be used for purposes other than login authentication, such as:

Biometric identification

Matches people to a database rather than having them perform identity verification themselves

Continuous authentication

Verifies that the logged-in user is still operating the device

Quick Check

You are designing a biometric authentication system and are considering retina scans. What concerns might others in your organization raise about using retina scans?

A. Retina scans may disclose information about underlying medical conditions.

B. Retina scans are painful as they require a puff of air in the user's eye.

C. Retina scanners are among the most expensive biometric devices available.

D. Retina scanners have a high false positive rate, leading to potential support issues.

Quick Check

Your organization is implementing a biometric system for high-security areas. In which scenario would they prefer a higher false rejection rate when compared to the false acceptance rate?

A. When security is more important than usability

B. When usability is more important than security

C. When the CER of the system is unknown

D. When the CER of the system is very high

Passwordless Authentication

Passwordless Authentication

It allows users to log into a system without entering a password or any other knowledge-based secret.

Users input their public identification and provide secure proof of identity through a registered device or token to complete the procedure.

Passwordless Authentication

Why passwordless?

Username and password are the most common yet most insecure form of authentication.

Over two-thirds of people reuse passwords across sites.

According to a 2023 report by IBM, 73% of data breaches involved compromised credentials, highlighting the ongoing risk of password-related security incidents.

Passwordless Authentication

Advantages

- Reduces risk by 99.9
- Adds an additional layer of protection with MFA
- Eliminates the need for a memorized secret

Passwordless Authentication

The user’s identity can be proved using an alternative factor, such as:

Something you have

Example

Cellular phone, OTP token, smart card, or hardware token

or

Something you are

Example

Fingerprints, retinal scans, or face and voice recognition

Passwordless Authentication: Benefits

- Eliminates the need for end users to create, manage, or remember passwords
- Highlights the fragility of passwords and their role in security violations, promoting passwordless security as a better option
- Reduces IT support costs since IT teams are no longer burdened by resetting forgotten passwords

Quick Check

Which passwordless authentication method should your company implement to enhance user experience on their online platform?

A. Magic links: Users receive email links for login
B. Biometric authentication: Users log in using fingerprint or facial recognition
C. One-time passcodes (OTP): Users enter a time-limited code sent via SMS or email
D. Social media login: Users authenticate using their social media credentials

Authorization and Accounting

Access Criteria

An organization should grant access privileges to subjects based on level of trust and need-to-know basis.

Access criteria include:

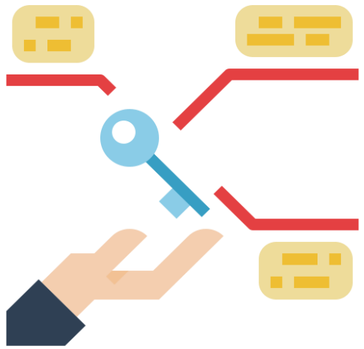
1. **Transaction:** Access is granted based on user privileges to perform specific commands and functions on data.
2. **Location:** Access is given based on the location of the user.
3. **Roles:** Access is granted depending on the role or job function in the organization.
4. **Time:** Access is permitted depending on the time of the day.
5. **Groups:** Access is authorized by creating user groups and assigning rights and privileges to the group.

Authorization Concepts

Need-to-know principle	Ensures that the subject is given access only to specific information depending on their job, duties, and requirements
Authorization creep	Occurs when an employee moves from one department to another and is assigned new access rights without reviewing and removing old permissions
Access control list (ACL)	Specifies the subjects granted access and the operations they are allowed to perform on objects
Default to zero	Starts with zero access, allowing the administrator to grant access based on the organization’s security policy

Least Privilege

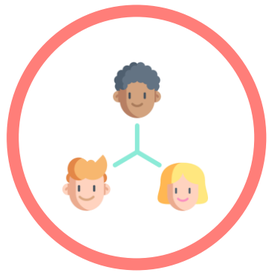
- It states that users should be given only the minimum access necessary to accomplish their tasks.
- It guarantees that users cannot execute any tasks that are not part of their allocated duties.



Example

Only less than 1% of Google employees get to set foot inside their data centers.

Separation of Duties (SoD)



- It is a principle that ensures that sensitive tasks are split into tasks performed by more than one person.
- It is an internal control that creates a system of checks and balances to prevent fraud and errors.

Accountability

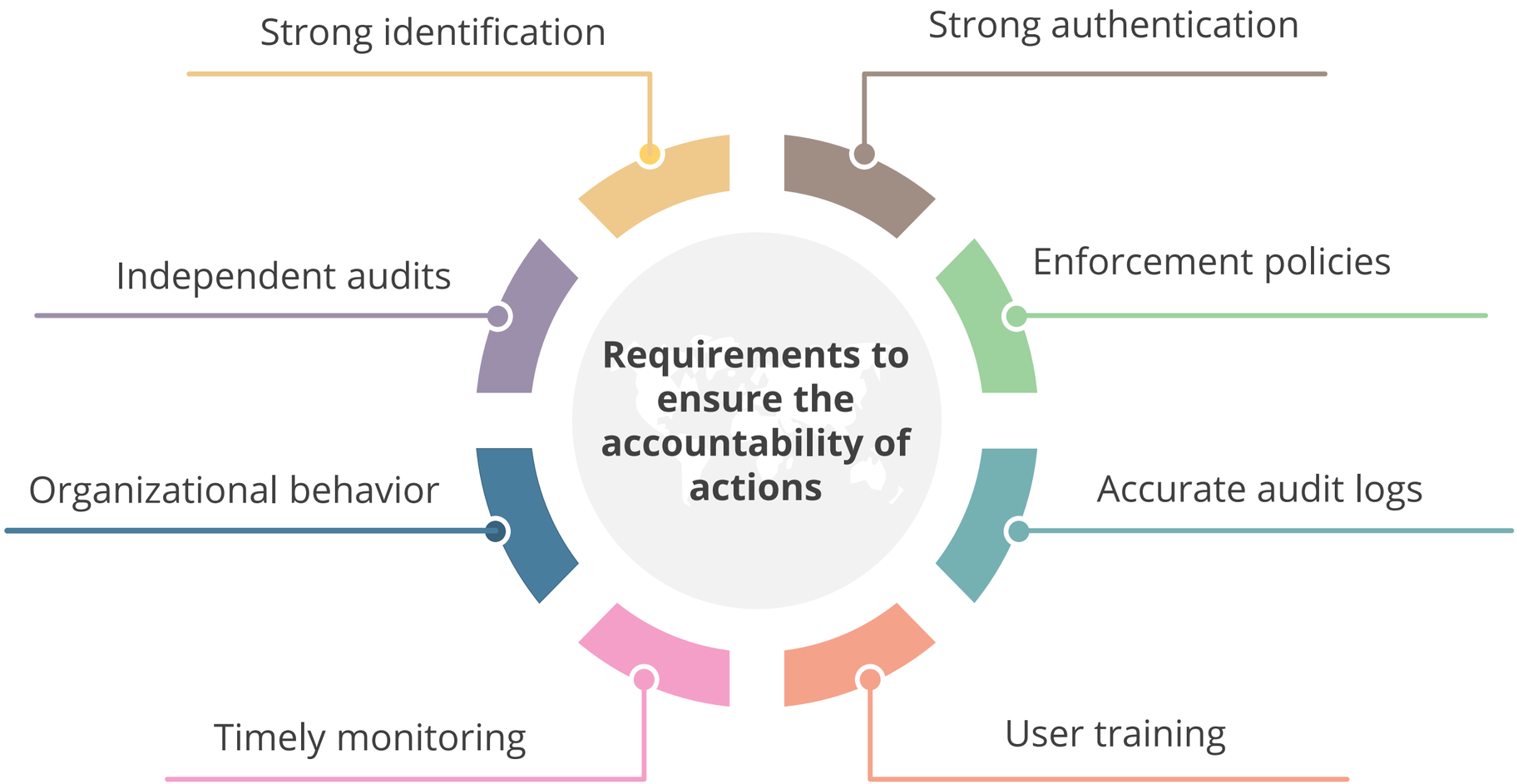
It ensures that users are responsible for their actions and enforces security policies.

It involves auditing and logging the following:

System-level events	Application-level events	User-level events
• System or computer performance • Successful and unsuccessful login attempts • Timestamps of the login attempts	• Error messages • File modifications	• Identification and authentication attempts • Commands used

Accountability

Non-repudiation ensures that users, processes, and actions are held accountable for their impacts.



Session Management

It is the way a single instance of identification, authentication, and authorization is applied to the entities.

Control and protection of desktop sessions can be achieved through:

- Screensavers
- Session or login limitation
- Timeouts
- Automatic logouts
- Schedule limitations

A session describes a single entity communicating with another for a specified period of time.

Credential Management Systems

It centralizes digital credentials, enhancing security and usability.

It integrates with various services, ensuring seamless logging, authentication, and access control, enhancing user experience.

Credential Management Systems

A security practitioner can build a good credential management system by incorporating the following:

- Password history
- Strong passwords
- Fast password retrieval
- Effortless password generation
- Well-defined access control
- Credential control
- Failover and redundancy
- Secure password storage
- Disaster preparedness
- Access tracking and auditing

Credential Management Systems: Risks and Benefits

Risks

- Attackers can compromise the credential management system.
- Reissuing credentials can be time-consuming and expensive.
- Compromise may lead to compliance issues.

Benefits

- It provides a high level of assurance.
- It meets the required security standards.
- It simplifies compliance, administration, and auditing.

Quick Check

A user is attempting to access a secure system. Which process evaluates whether the user can be trusted for the specific access they are requesting?

A. Authorization

B. Authentication

C. Identification

D. Accounting

Federated Identity Management

Federated Identity

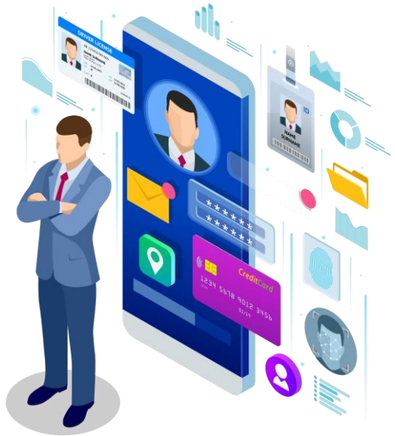
It is a portable identity that, along with its associated entitlements, can be used across business boundaries.

- It authenticates a user across multiple IT systems and enterprises.
- It links a user’s distinct identities at various locations without synchronizing or consolidating directory information.

Federated Identity Management (FIM)

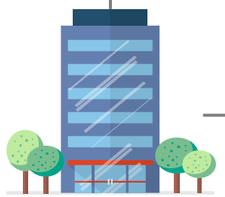
It addresses the identity management issues that arise when multiple organizations need to share the same applications and users between them.

- It requires each organization to adhere to common policies, standards, and procedures for managing user identification, authentication, and authorization.
- It establishes a trust relationship among participating organizations.



FIM: Example

John is authenticated
to company A



John is authenticated
to company B

John is authenticated
to company C

John is authenticated
to company D

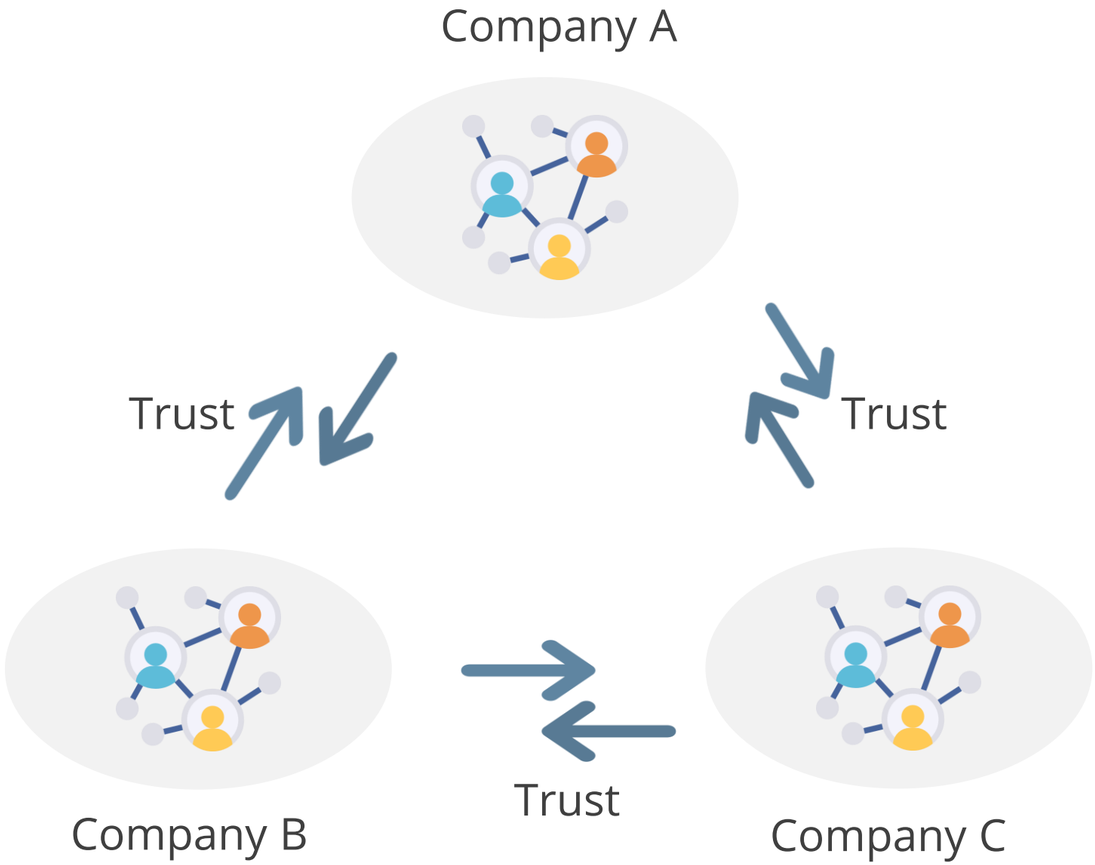
Assertions

If a user logs into Expedia to book a hotel room, they might be redirected to the Hilton website, where Expedia automatically transfers the user's login details to Hilton.

FIM: Types

Cross certification model

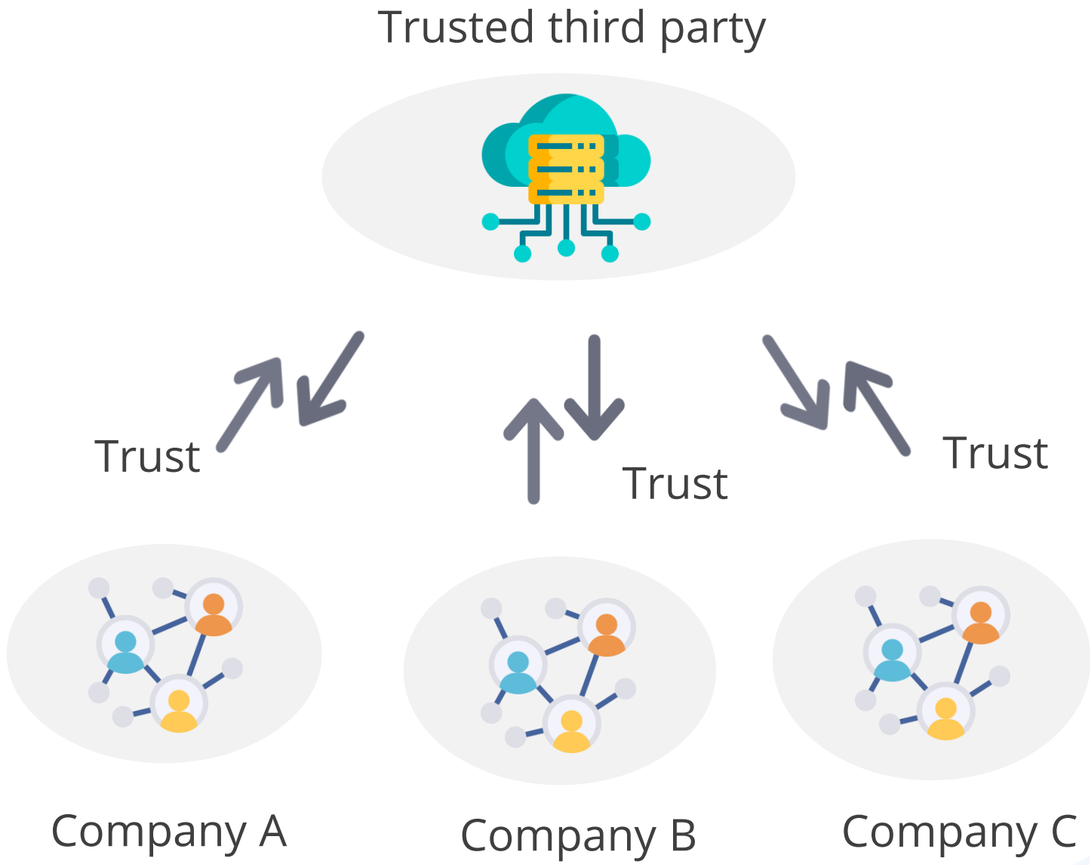
- Certifies every other participating organization
- Manages trust relationships, which becomes difficult as the number of participating organizations increases
- Plays the roles of both identity provider and service provider, depending on the communication



FIM: Types

Trusted third party

- Subscribes to the standards and practices of a trusted third party that manages the verification and due diligence process for all participants
- Considers the participating organizations trustworthy after verification by the third party
- Acts as a trusted entity or bridge between participating organizations for identity verification purposes
- Serves as the identity provider in the trusted third-party certification model, with other organizations serving as service providers



Federation Identity Management Standards

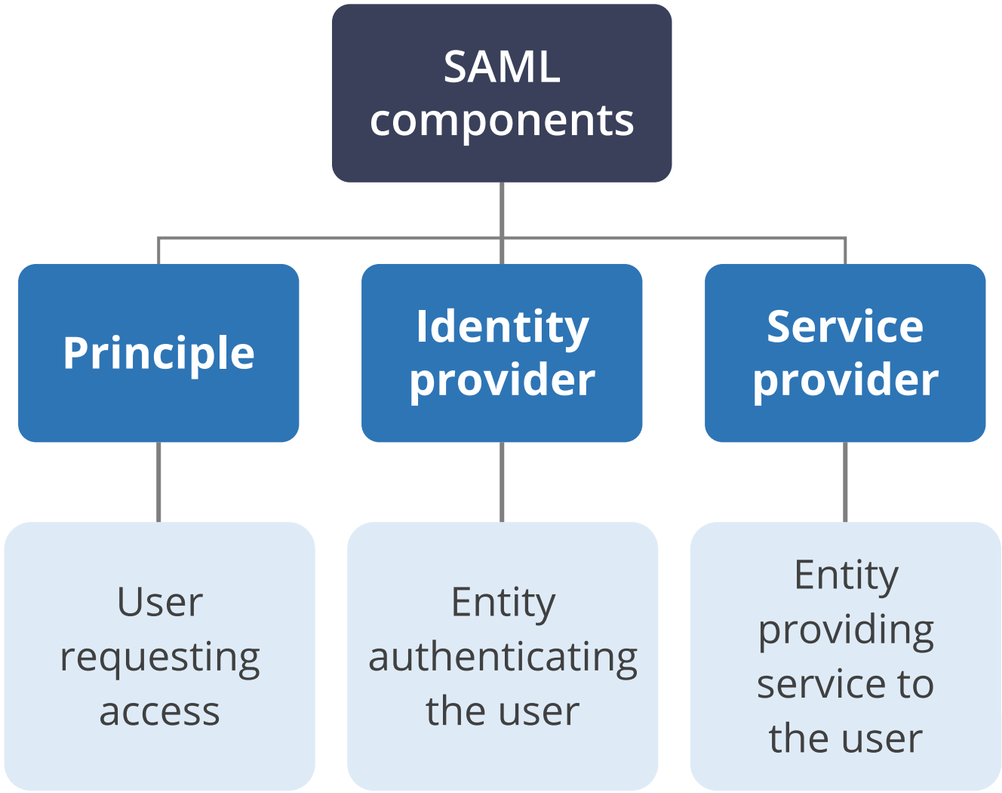
Federation Identity Management Standards

FIM relies on several key standards to ensure interoperability and security.

Security Assertion Markup Language (SAML)

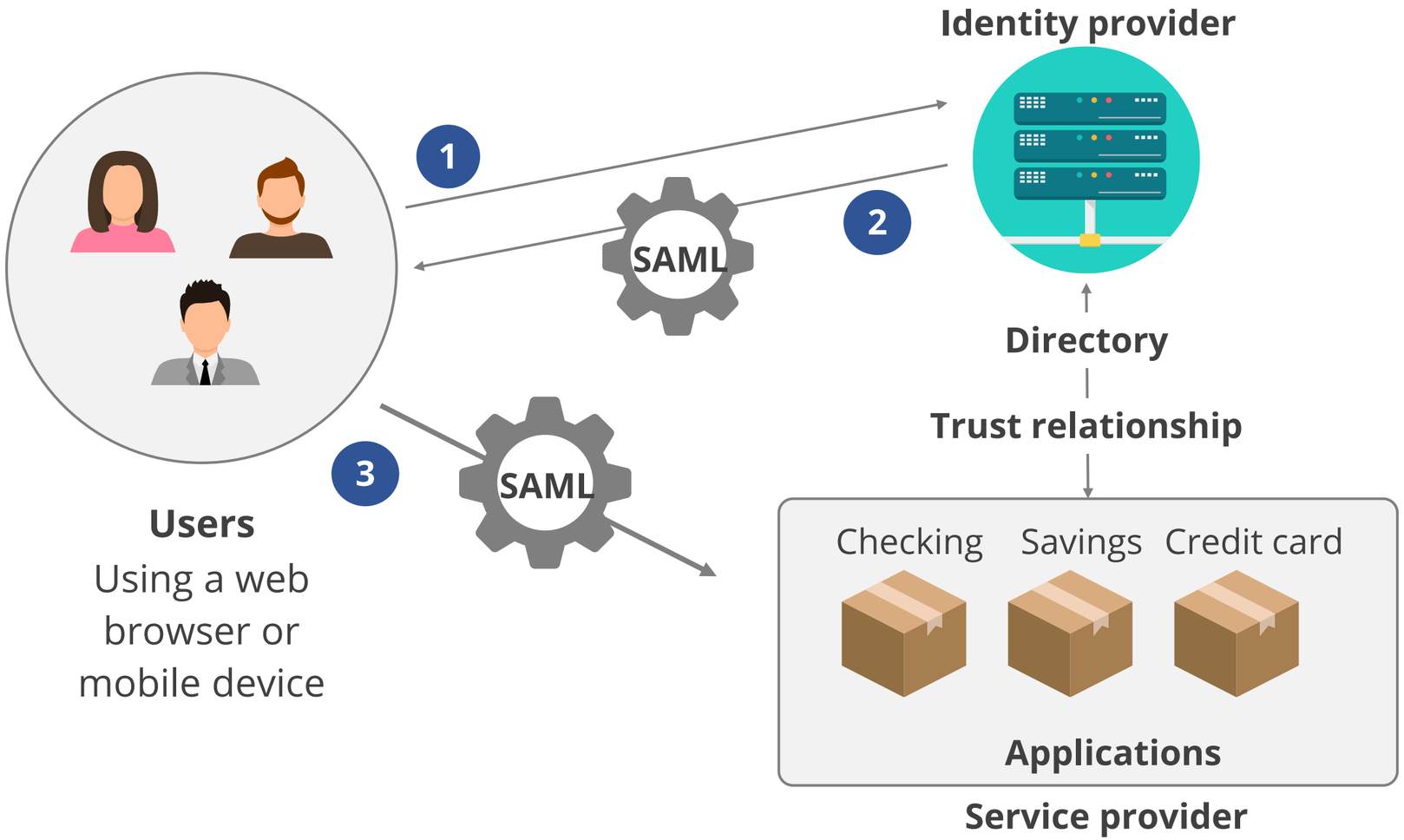
It is an XML standard that allows the exchange of authentication and authorization data between security domains.

- Provides the authentication pieces to the federated identity management systems
- Uses SAML and SPML for the exchange of authentication and authorization or provisioning data among federated identity systems
- Offers SSO capabilities to access different browsers
- Relies on TLS for message confidentiality and digital signatures for message integrity, lacking a security mode



Security Assertion Markup Language (SAML)

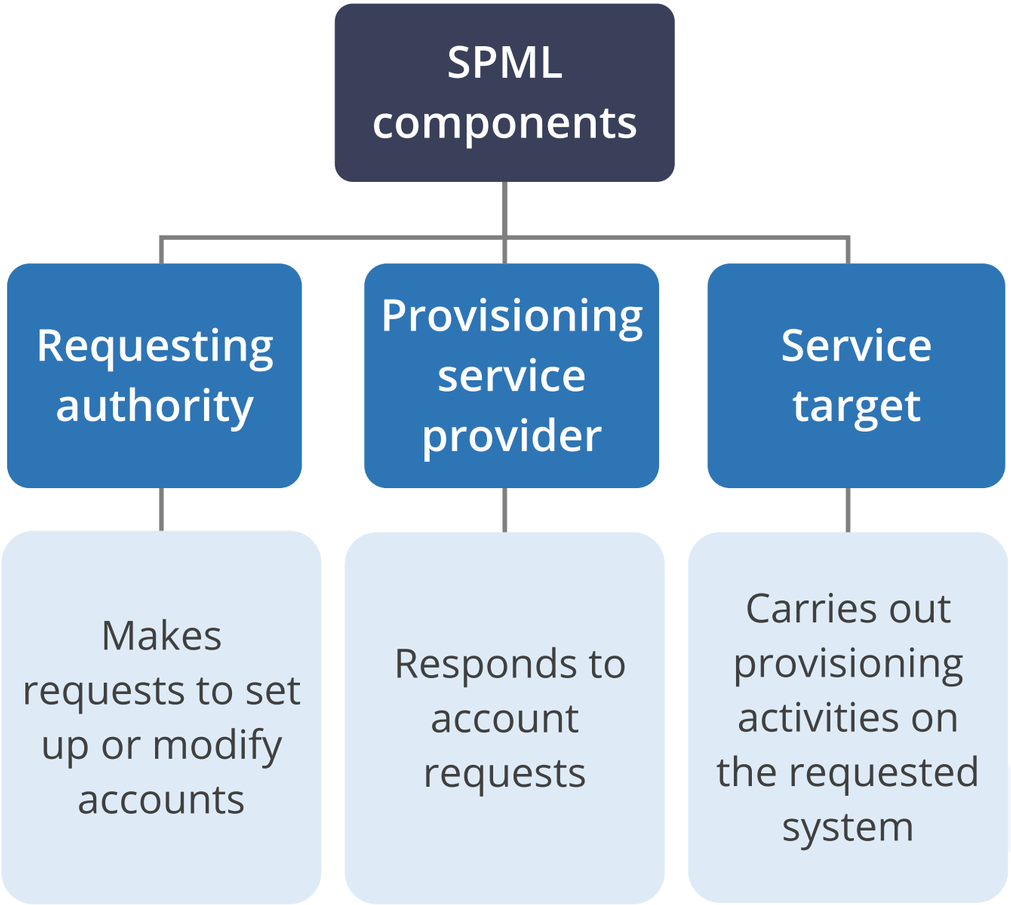
The diagram below shows the working of SAML:



Service Provisioning Markup Language (SPML)

It helps exchange provisioning data between applications within one organization or across different organizations.

- Automates user management and access entitlement configuration across multiple provisioning systems
- Integrates and interoperates service provisioning requests across various platforms



OpenID Connect

It allows the use of an existing account to sign in to multiple websites without needing to create new passwords.

- Enables sharing of information like name or email address with the websites visited, while controlling the amount of information shared
- Ensures that only the identity provider receives the password, which then confirms the identity to the websites visited
- Prevents other websites from ever seeing the password, eliminating the risk of compromising the identity on unscrupulous or insecure websites

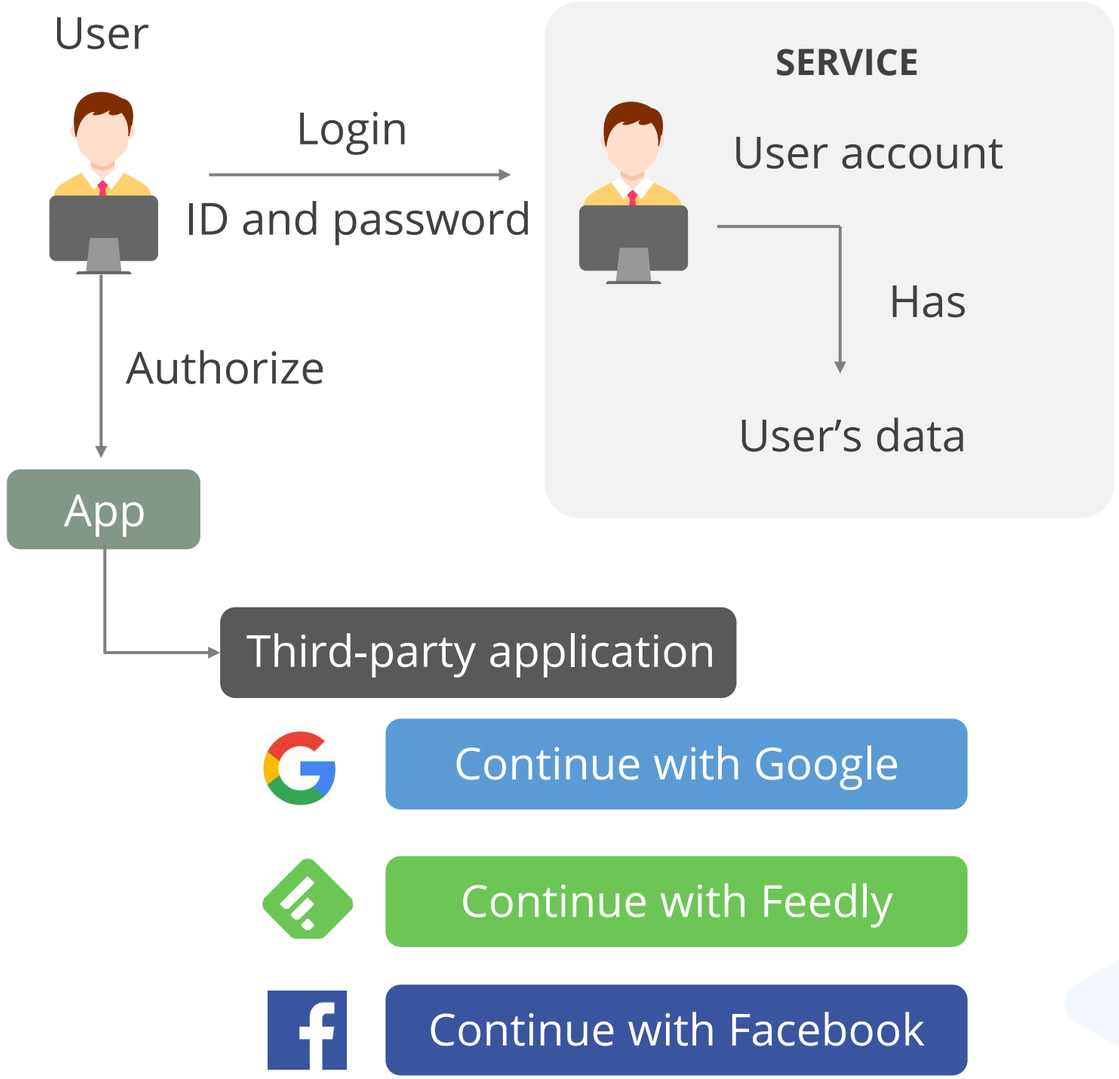
OAuth

It is an open-standard authorization protocol that enables unrelated servers and services to safely access their assets without sharing the initial, related, and single login credentials.

This is known as secure, third-party, user-agent, and delegated authorization.

OAuth

- **Example**: A user logs into a website using credentials from another service.
- The user clicks the link to the other website that authenticates the user.
- The original website logs the user using the permission obtained from the second website.



Difference between SAML, OAuth, and OpenID

	SAML 2.0	OAuth2.0	OpenID connect
Purpose	Authorization and authentication	Authorization	Authentication
History	Developed by OASIS in 2001	Developed by Twitter and Google in 2006	Developed by the OpenID Foundation in 2004
Data format	XML	JSON	JSON
Use case	SSO for enterprise applications	-	SSO for consumer applications

Identity as a Service (IDaaS)

It is a SaaS-based IAM solution built and operated by a third-party provider. It is provided as a subscription-based service.

The key features of IDaaS are:

User management and access control

Provides administrative tools for onboarding users and managing their access privileges throughout the course of their employment

Multi-factor authentication (MFA)

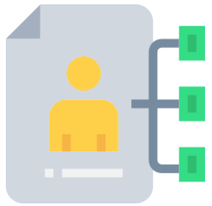
Requires users to submit multiple factors to access their resources, providing greater security than single-factor authentication (username and password)

Single sign-on (SSO)

Enables users to access all their business applications and services using a single set of login credentials

Identity as a Service (IDaaS)

Most organizations rely on Microsoft Active Directory Domain Services (AD DS) to provide a unified system to manage identities to ensure consistency and administrative efficiency.



Active directory can be federated with a third-party IDaaS provider, such as Okta and Ping Identity, to provide a hybrid identity solution that integrates cloud services with on-premise capabilities.

A unified identity management system minimizes administrative effort in managing accounts and controlling access and provides a single end-user authentication process across a hybrid environment.

Quick Check

You are looking for an open standard for cloud identity federation that utilizes XML's flexibility for authentication, authorization, and attribute information. Which standard should be adopted to achieve this?

A. SAML

B. SOAP

C. OAuth

D. OpenID Connect

Single Sign-On

Single Sign-On (SSO)

This technology allows users to log in to multiple applications with just one set of credentials.

- The user only needs to enter credentials once to access all the corporate resources to which they are entitled.
- **Analogy:** Imagine having a master key for a house that unlocks all the doors. SSO is like that for the digital life.

Single Sign-On (SSO)

Pros
It needs only one password for all enterprise systems and applications.
It requires only one strong password to be remembered and used.
It allows user accounts to be easily created on hire and modified or deleted on dismissal.

Cons
It is difficult to implement.
It can be a reason for centralized point of failure.
It can lead to potential data compromise.

Single Sign-On (SSO)

It uses the following technologies:

Kerberos	SESAME	Dumb terminal (Thin client)	Script-based sign-on
This protocol uses a key distribution center, tokens or tickets, and symmetric key cryptography.	The Secure European System for Applications in a Multivendor Environment (SESAME) authentication protocol uses asymmetric cryptography.	It depends on a central server for access control, processing, and storage.	It is an SSO solution that is implemented by an organization through the development of a script.

Kerberos

It is an authentication protocol that offers a single sign-on solution for distributed environments.

It uses a client/server model based on tickets to allow nodes to securely interact on an insecure network and confirm their identity to one another.

Key Features of Kerberos

Single sign-on: It is an open protocol that allows users to authenticate only once to access multiple resources within its realm.

Strong encryption: It uses advanced encryption standard (AES) symmetric-key cryptography to protect data confidentiality and integrity.

Mutual authentication: It authenticates both the client and the server, ensuring the identity of both parties.

Key Features of Kerberos

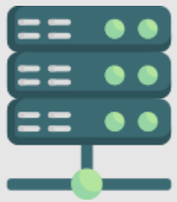
Ticket-based authentication: It uses tickets for access, reducing password transmission.

Centralized management: It utilizes a key distribution center (KDC) which allows centralized management of user credentials and ticket issuance.

Scalability: It handles large numbers of users and services.

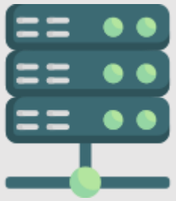
Key Distribution Center (KDC)

It is a central authentication server in the Kerberos protocol, responsible for issuing tickets that allow users to access network services.



Authentication service (AS)

Ticket granting service (TGS)



- AS is the first component in the Kerberos and handles initial authentication.
- AS verifies user credentials and issues a ticket granting ticket (TGT) to authenticate the client.
- TGS validates TGT and issues service tickets, which are used for accessing the services.

It is a trustworthy third party that offers authentication services.

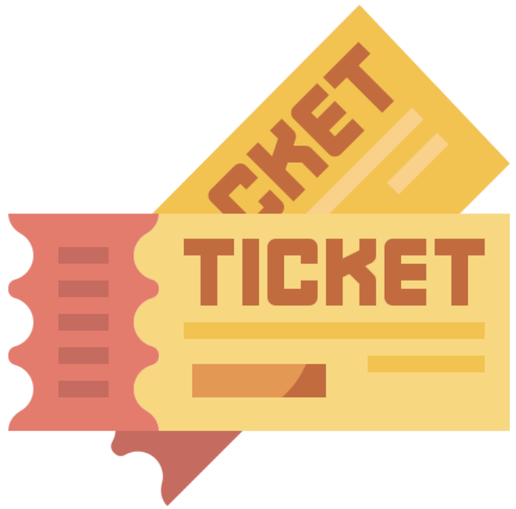
Ticket-Granting Ticket (TGT)

When seeking tickets to access objects, subjects present the TGT.

- It verifies that a subject has been verified by a KDC and is authorized to request tickets for access to other objects.
- It contains a symmetric key, an expiry period, and the user's IP address, and is encrypted with the TGS secret key.

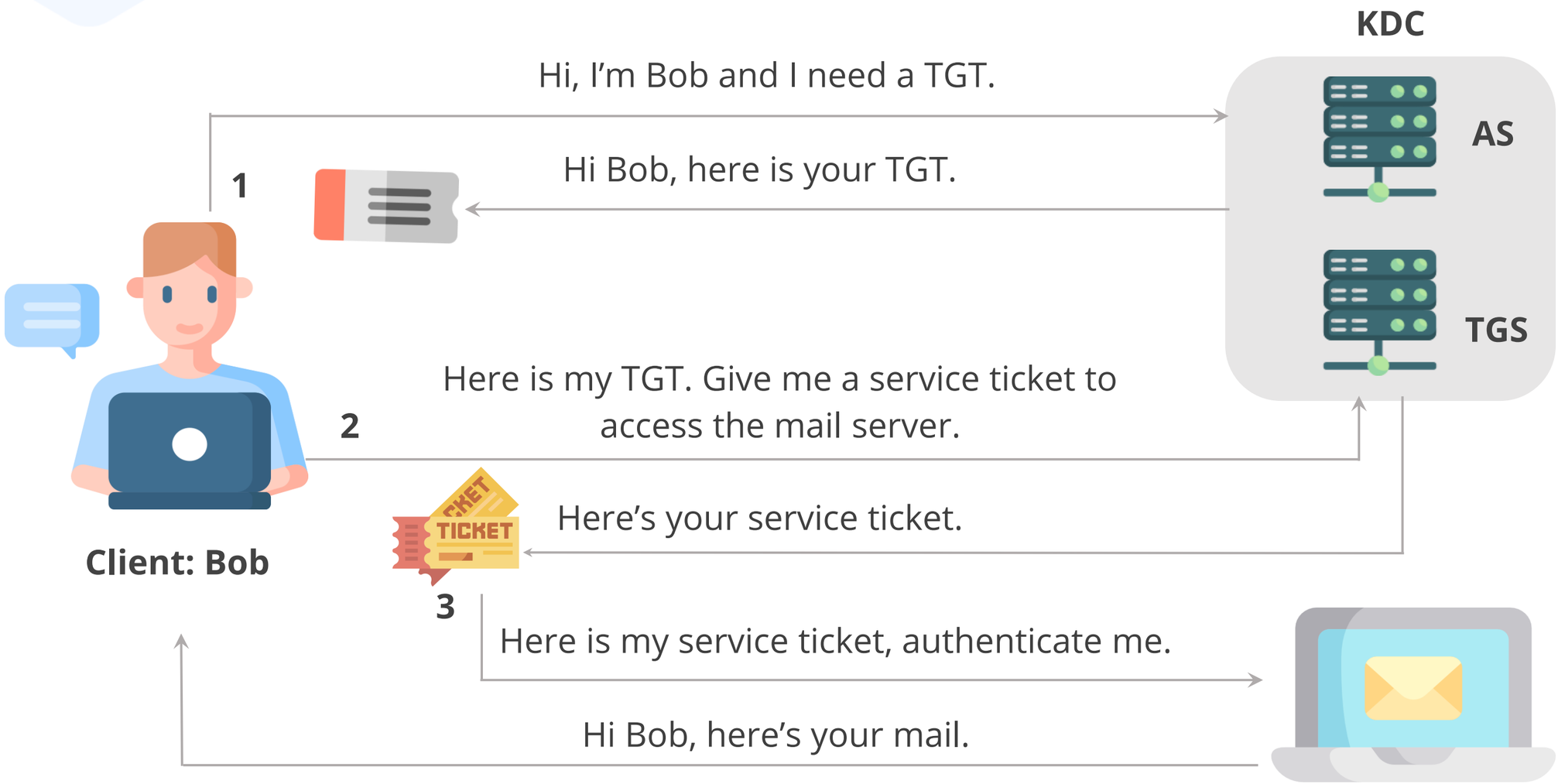
Service Ticket

It is an encrypted message that proves a subject is authorized to access an object.



- Kerberos issues service tickets to subjects who seek access to objects.
- Kerberos service tickets feature a set of lifetime and usage constraints.
- The client must request a renewal or a new service ticket to continue communicating with any server after the current ticket expires.

Kerberos Authentication Process



Weakness of Kerberos

- Can be a single point of failure
- Can be vulnerable to password guessing
- Can lead to the compromise of the secret key for every system on the network if compromised
- Requires all client and server clocks to be synchronized within five minutes

Difference between FIM and SSO

Federated identity management (FIM)	Single sign-on (SSO)
Enables a single credential to access multiple applications and resources across multiple organizations	Allows a single credential to access multiple applications and resources within one organization
Provides SSO	Does not necessarily provide FIM

Quick Check

During the client authentication process in Kerberos, what does the client send to the authentication server (AS)?

A. Only cleartext message of the user ID

B. Encrypted user ID and password

C. Encrypted user ID, password, and secret key

D. Cleartext user ID and encrypted password

Privilege Access Management

Privileged Access or Account Management (PAM)

It is a cybersecurity strategy that aims to secure access to vital systems and resources within an organization’s IT environment.

- It is also known as privileged identity management (PIM).
- Privileged accounts have elevated permissions that allow them to make significant changes to systems and data.
- If compromised by unauthorized users, the damage can be severe.

Just-in-Time (JIT) Access Control

It is a security practice that grants users elevated privileges only when necessary for a specific task and for a limited period.

- It is a cornerstone of PAM and aligns with the principle of least privilege.
- It can help organizations significantly enhance their security posture and protect sensitive data.

Just-in-Time (JIT) Access Control

It enables organizations to grant users on-demand and privileged access to applications or systems for a predetermined period on an as-needed basis.

It verifies requests against a pre-approval policy or allows reviews by an administrator who can grant or deny requests for short-term privileged access.

It facilitates access using ephemeral certificates for temporary and secure authentication.

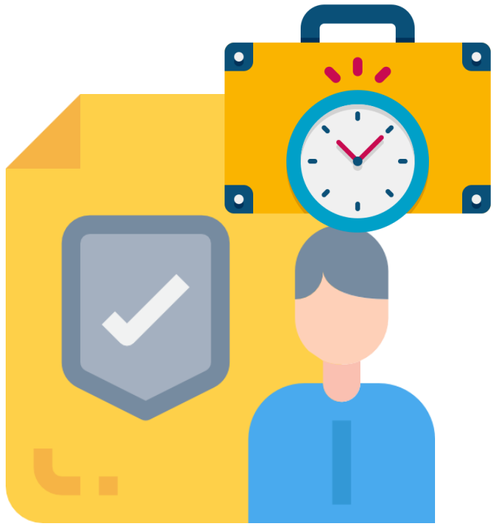
It enforces the security principle of least privilege by providing users the least amount of access to perform the required job for the minimum duration necessary.

Source: www.centrify.com/pam/privilege-elevation/

Ephemeral Credentials

These are temporary access keys that offer extra security by minimizing the window of opportunity for attackers.

- They are short-term, one-time-use credentials often used by IT administrators for specific projects.
- These credentials are secure because they only work for a limited time, making it difficult for attackers to exploit them.

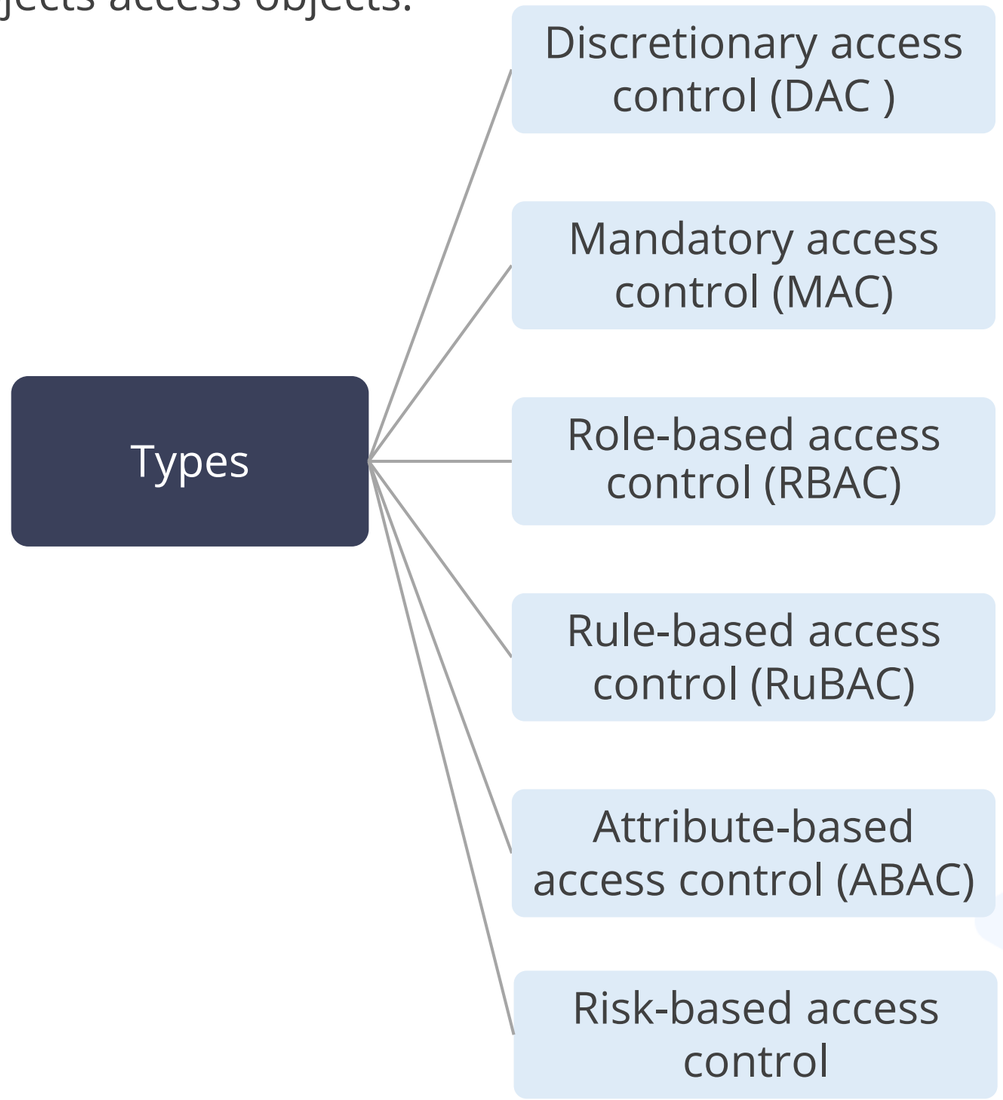


Implement and Manage Authorization Mechanisms

Access Control Model

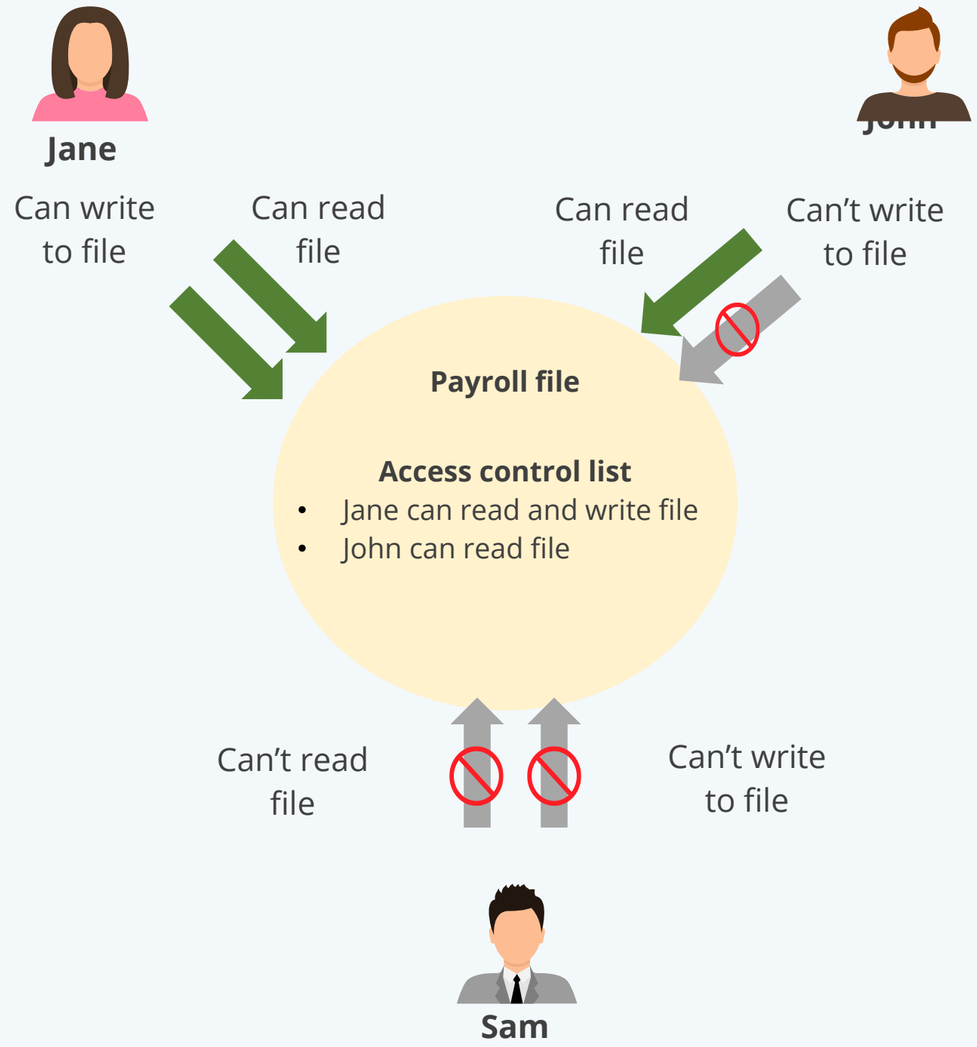
It is a framework that dictates how subjects access objects.

- Each model type uses different methods to control how subjects access objects.
- An organization's business and security goals determine what access control model they should use.
- The models are built into the core or the kernel of different operating systems and possibly their supporting applications as well.
- They guide the way a subject accesses an object.



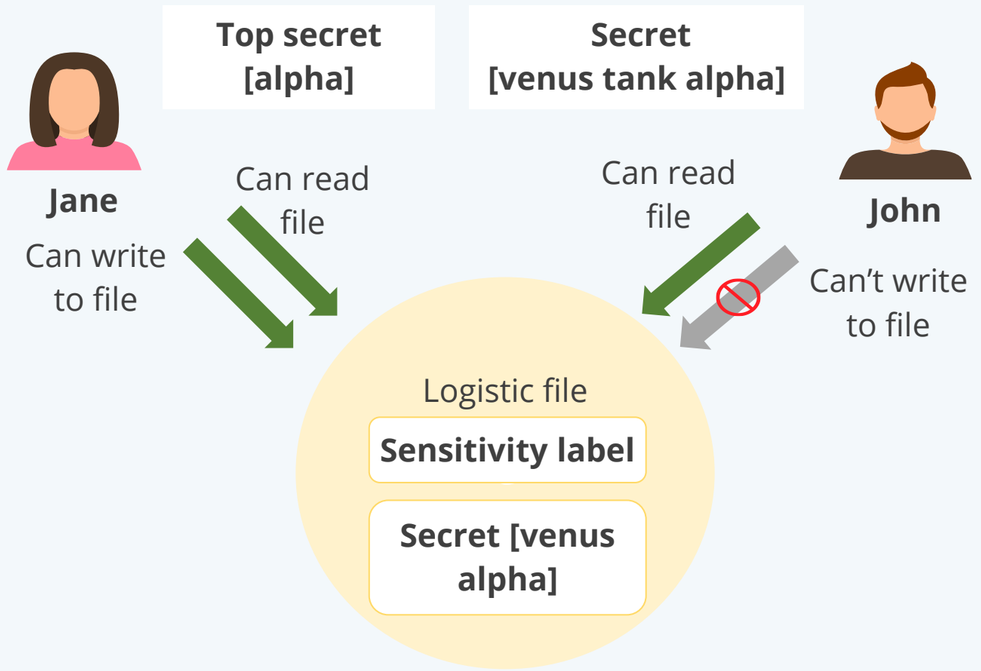
Discretionary Access Control (DAC)

- Access to resources is determined by data owners.
- Access control depends on the owner's discretion and the authorization granted to users.
- Access control lists (ACLs) are used to enforce the security policy.



Mandatory Access Control (MAC)

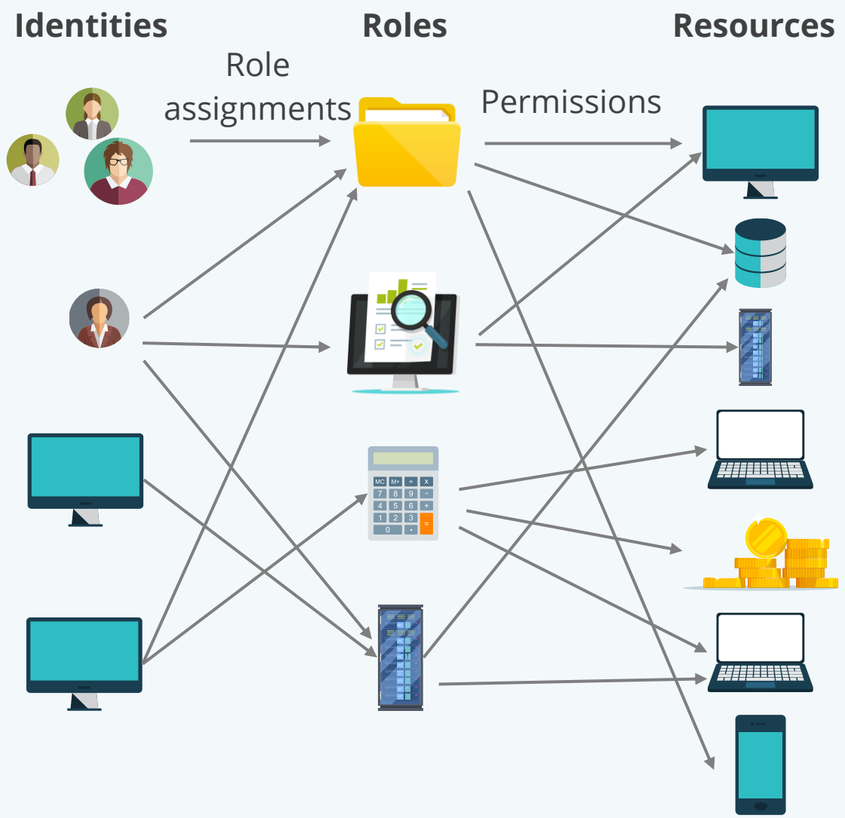
- The system’s security policy is enforced by the operating system using security labels.
- Resources have security labels containing data classification, and the users have security clearances.
- This model is used when information classification and confidentiality are important.



Role-Based Access Control (RBAC)

It is a widely used approach to restricting access to computer systems and networks.

- Defines different roles within a system and assigns permissions to those roles
- Assigns roles to users based on their job functions or needs
- Simplifies access management and ensures that users only have the access they need to perform their jobs

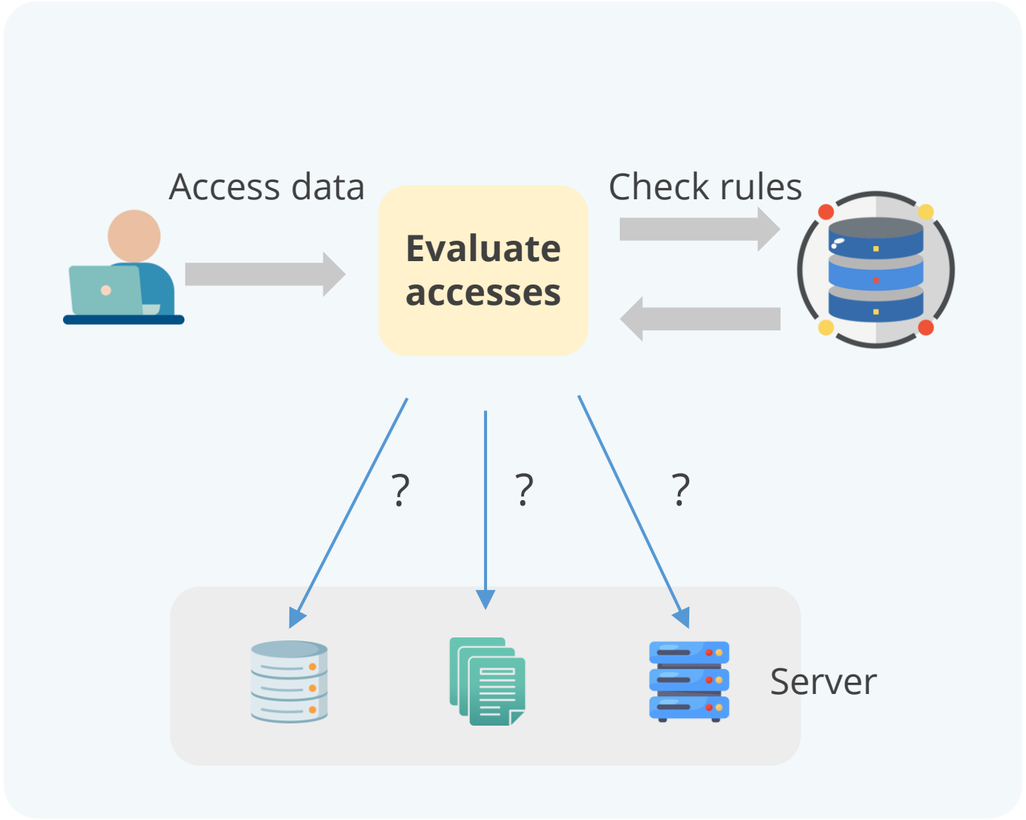


Rule-Based Access Control (RuBAC)

Access requests are evaluated against predefined rules that determine the access to be granted.

The rules are in the form of *if* or *then statements.*

They can be applied to all users or subjects regardless of their identities.



Example

Routers and firewalls use rules to filter incoming and outgoing traffic within an ACL, as defined by an administrator. The firewall examines all traffic and only allows traffic that meets one of the rules.

Attribute-Based Access Control (ABAC)

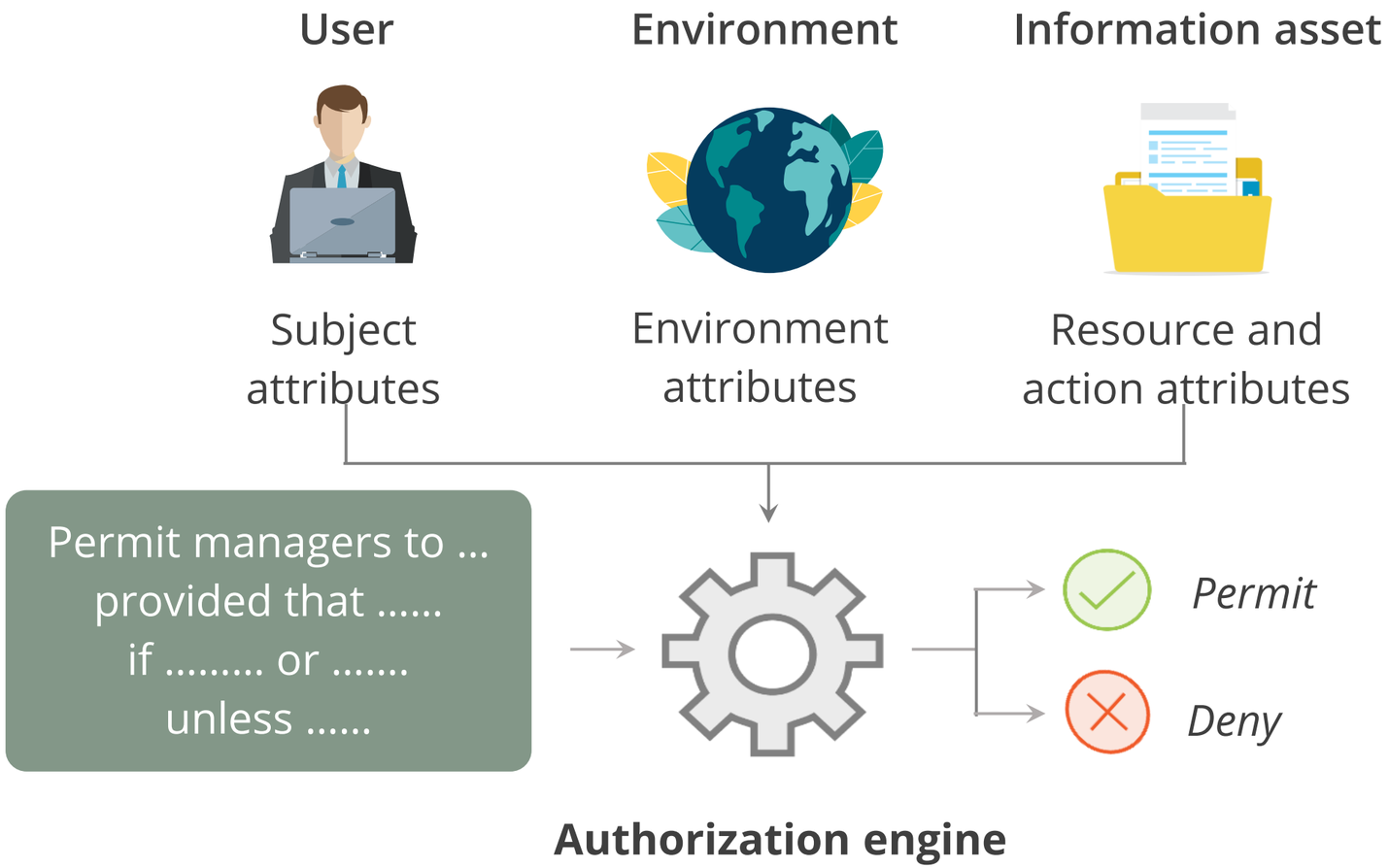
An access control method where requests to perform operations on objects are granted or denied based on attributes of the subject, attributes of the object, environment conditions, and specified policies
~ NIST

Granular policies can be established by combining these attributes to grant or deny access.

Attributes provide details for building authorization policies, such as who wants access to what, from where, when, and why.

Attribute-Based Access Control (ABAC)

The following diagram describes the ABAC principle:

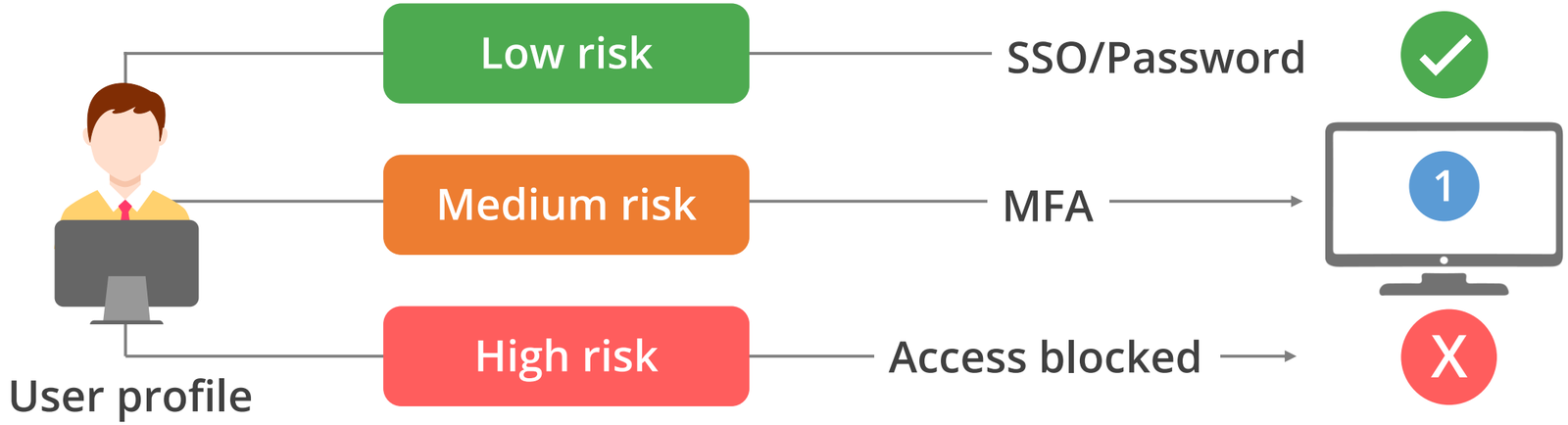


RBAC vs. ABAC

	Role-based access control	Attribute-based access control
Access	Access is based on roles	Access is based on attributes
Distributed environment	Not ideal when subject and resource belong to different security domains	Ideal to handle complex distributed environments
Environment attributes	Does not consider environment attributes explicitly	A new rule involving an environment attribute can be easily added
MAC	Does not handle MAC	MAC security labels can be treated as attributes
Complexity	Can handle simpler scenarios	Can handle complex scenarios where contextual information needs to be evaluated
Cost	Cheaper than ABAC	More costly to implement and maintain

Risk-Based Access Control

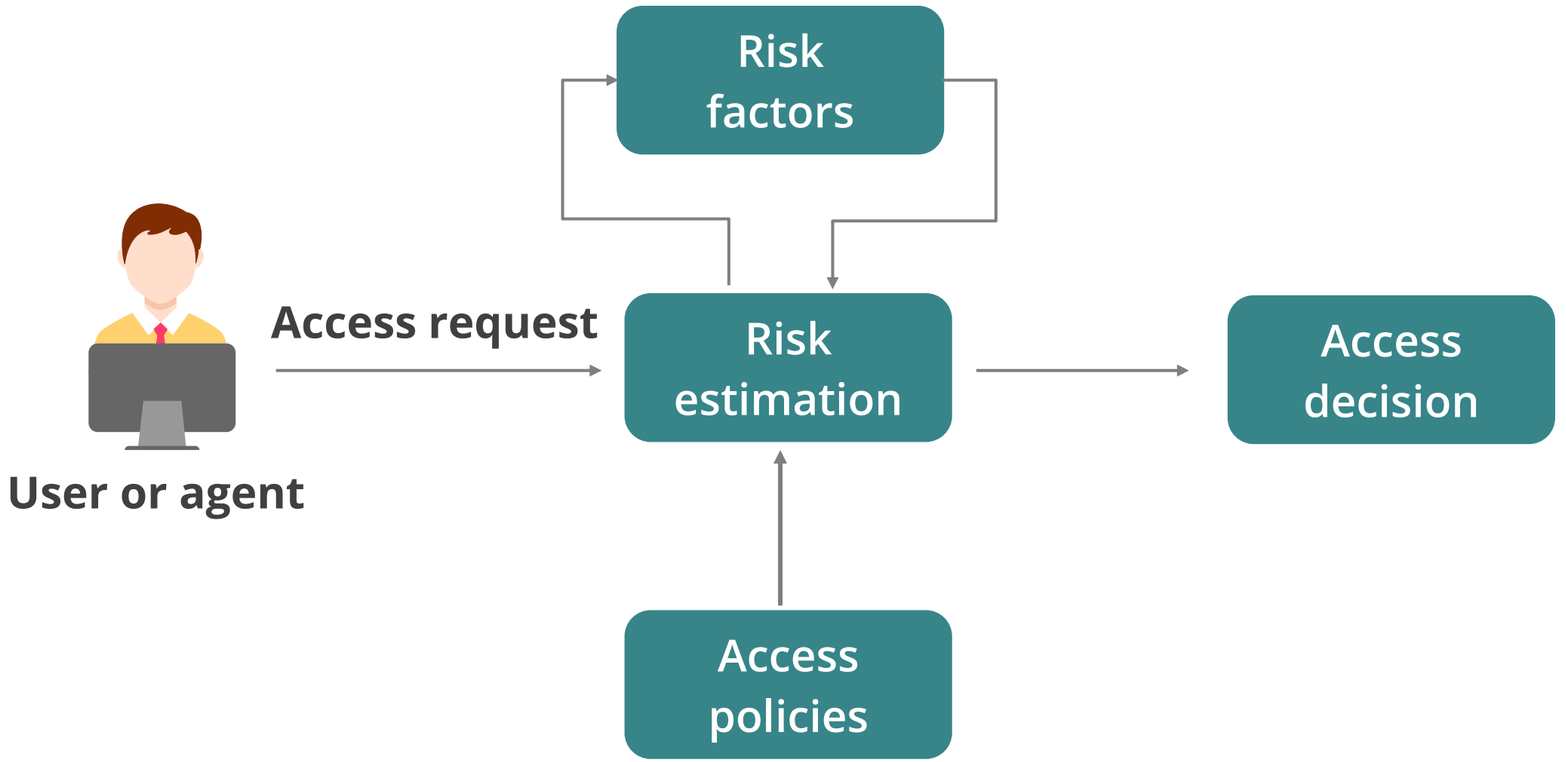
This is a dynamic authentication method that considers the security risk value related to each access request as a criterion to determine access decisions.



- Users authenticating from known devices, locations, and networks with a low-risk score could be automatically signed in.
- Suspicious users are required to provide additional credentials using MFA.
- Access requests with a high-risk score would be denied.

Risk-Based Access Control

The main elements of risk-based access control include:



Access Control Tools and Techniques

Access Control Tools and Techniques

These tools allow one to control flows between subjects and objects through different method.

01 Access control matrix

02 Constrained user interface

03 Content-based access control

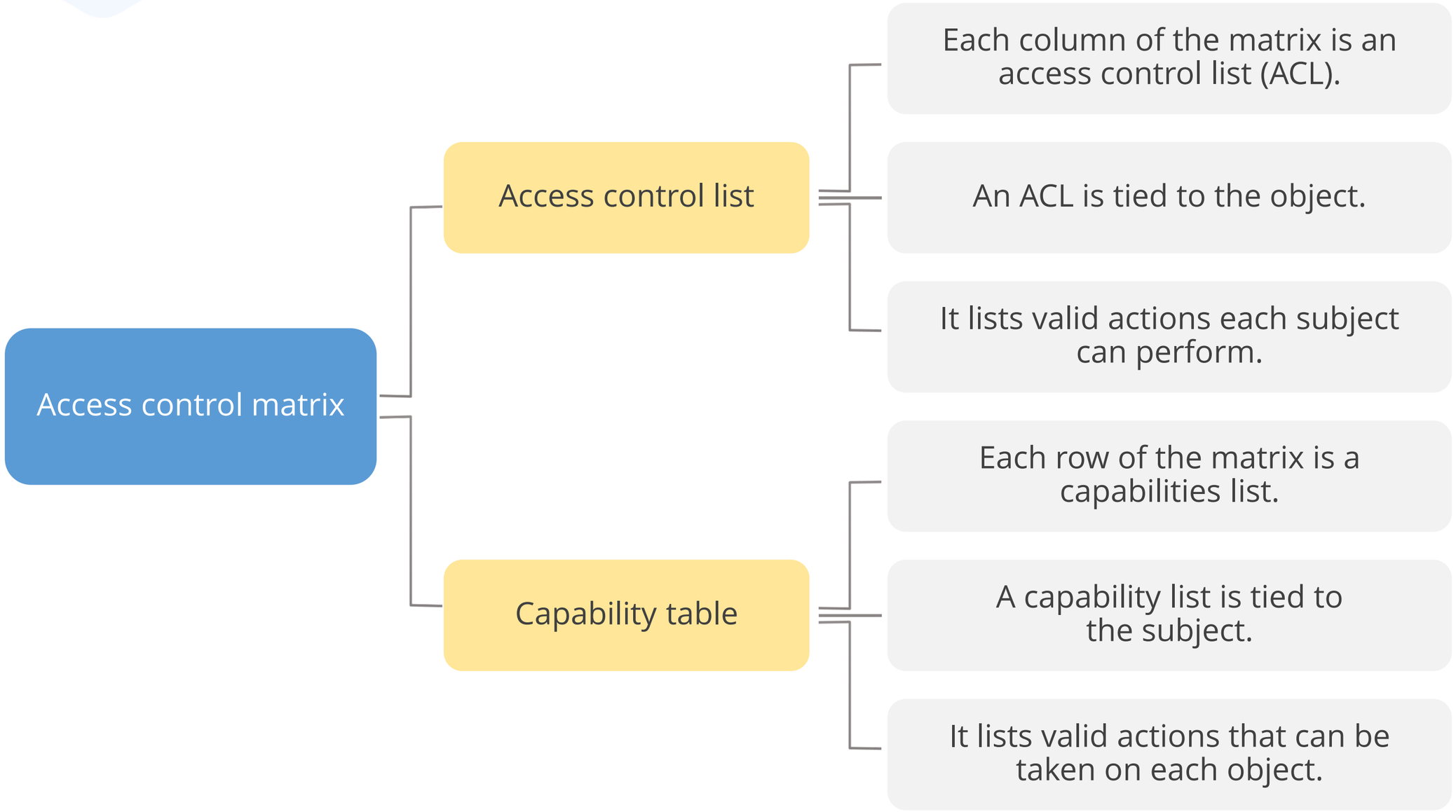
04 Context-based access control

Access Control Matrix

It is a table of subjects and objects that indicate the actions or functions that each subject can perform on each object.

Subject	CISSP	CISA	CRISC	CISM
Alex	Read	Write	Read	Write
Peter	Write	No access	Write	No access
John	No access	Read, write	No access	Read, write
Bob	Read, write	Read	Read, write	Read

Access Control Matrix



Constrained User Interface

It is a security mechanism that restricts a user's interaction with an application or system.
Some of its components include:

Menus

Provides users with limited options to execute

Shells

Contains only the commands the administrator wants the user to be able to execute

Database views

Restricts user access to data contained in databases

Physical constraining

Provides only certain keys on a keypad or certain touch buttons on a screen to implement constrained interface

Content-Based Access Control

- Access to objects is determined by the content within the object
- Employed on content-dependent devices

Example

URL-based filtering and email filtering

Context-Based Access Control

- Makes access decisions based on the context of the collection of information rather than on the sensitivity of the data
- Reviews the previous actions or the current situations and then takes the decision

Example

Stateful firewall and time-based access control

Quick Check

When users login to their banking application from overseas, they are required to provide additional credentials based on the risk score generated by their behavior. This is an example of:

A. Mandatory access control

B. Risk-based access control

C. Attribute-based access control

D. Behavior-based access control

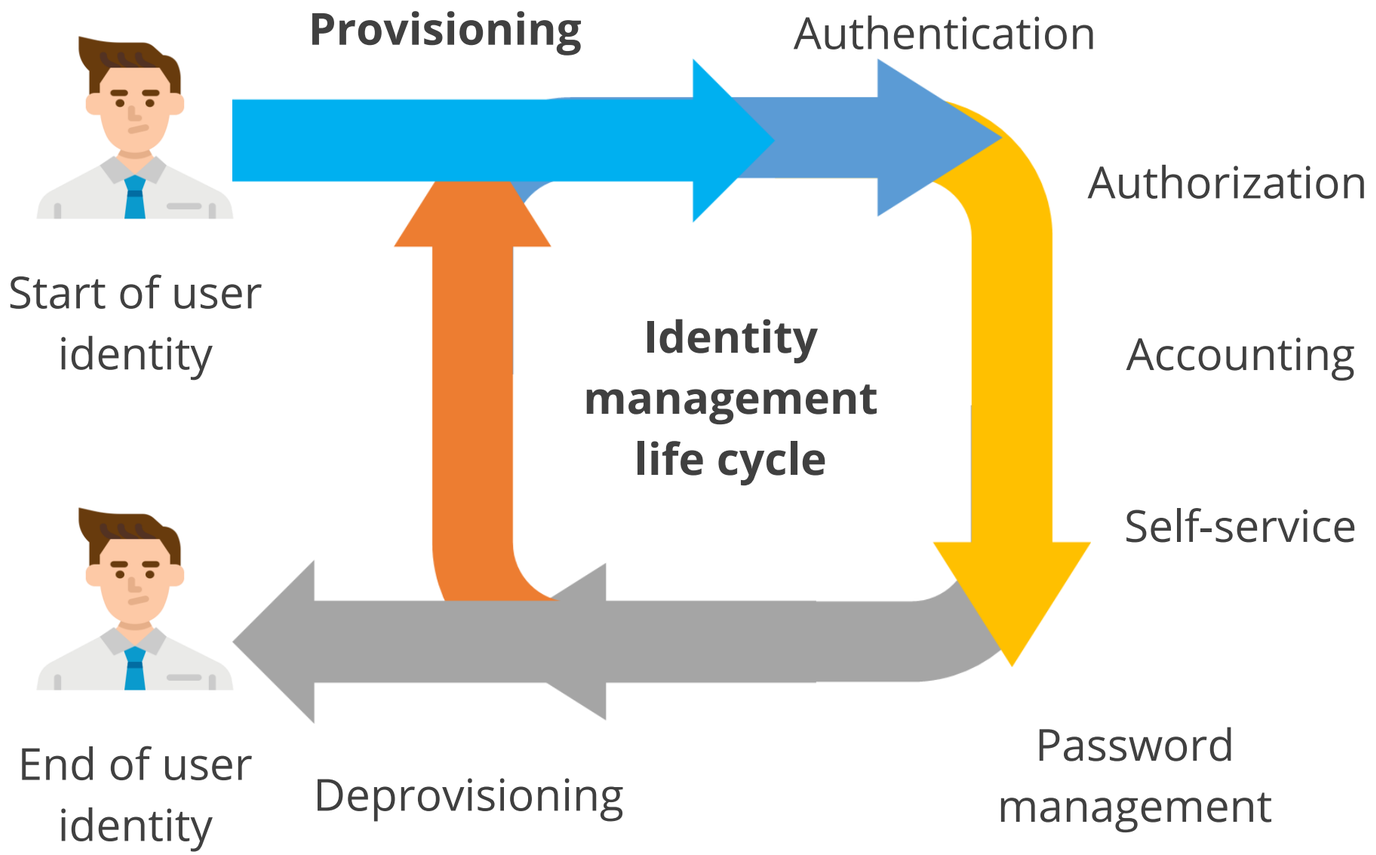
Manage the Identity and Access Provisioning Lifecycle

Identity Proofing

It confirms a person's identity to ensure the authenticity and legitimacy of their actions.

- Acts as a foundational step in identity and access management, helping organizations prevent fraudulent activities
- Requires presenting certain forms of evidence such as a passport, driver's license, or social security number (SSN) for identification

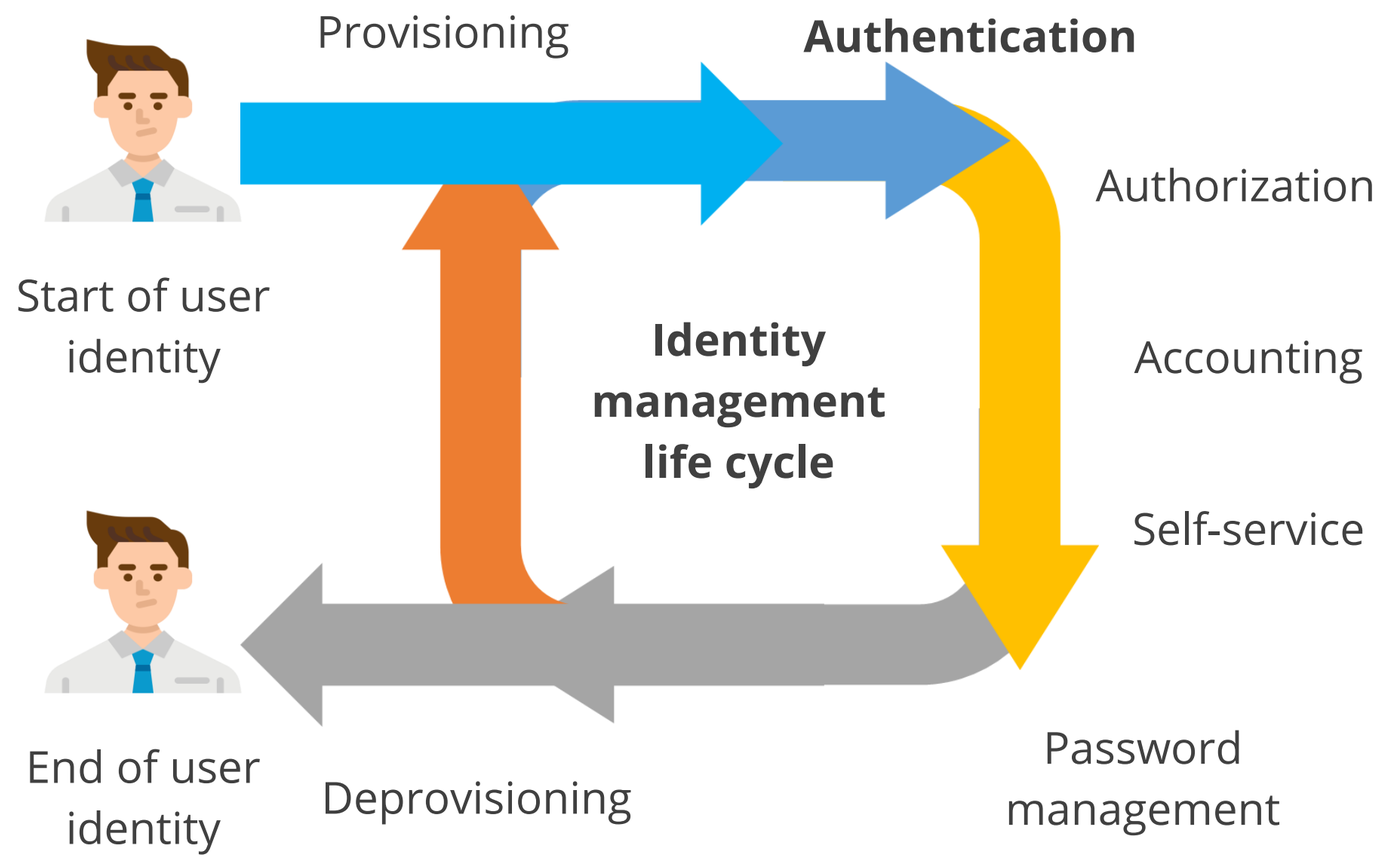
Identity Management Life Cycle



Provisioning

- Create person and identifier
- Define their group and role membership
- Define systems and accounts required

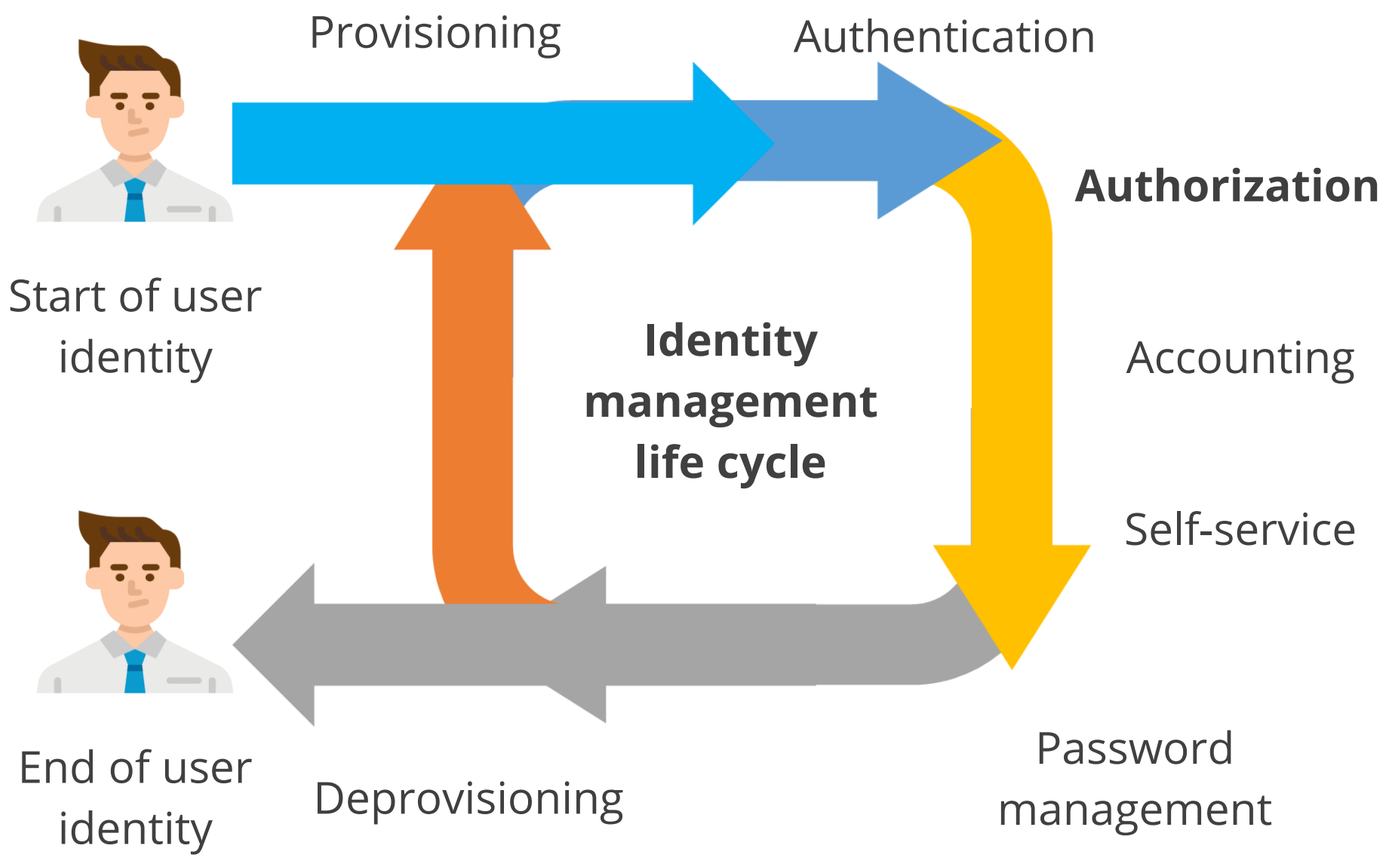
Identity Management Life Cycle



Authentication

Validate user identity

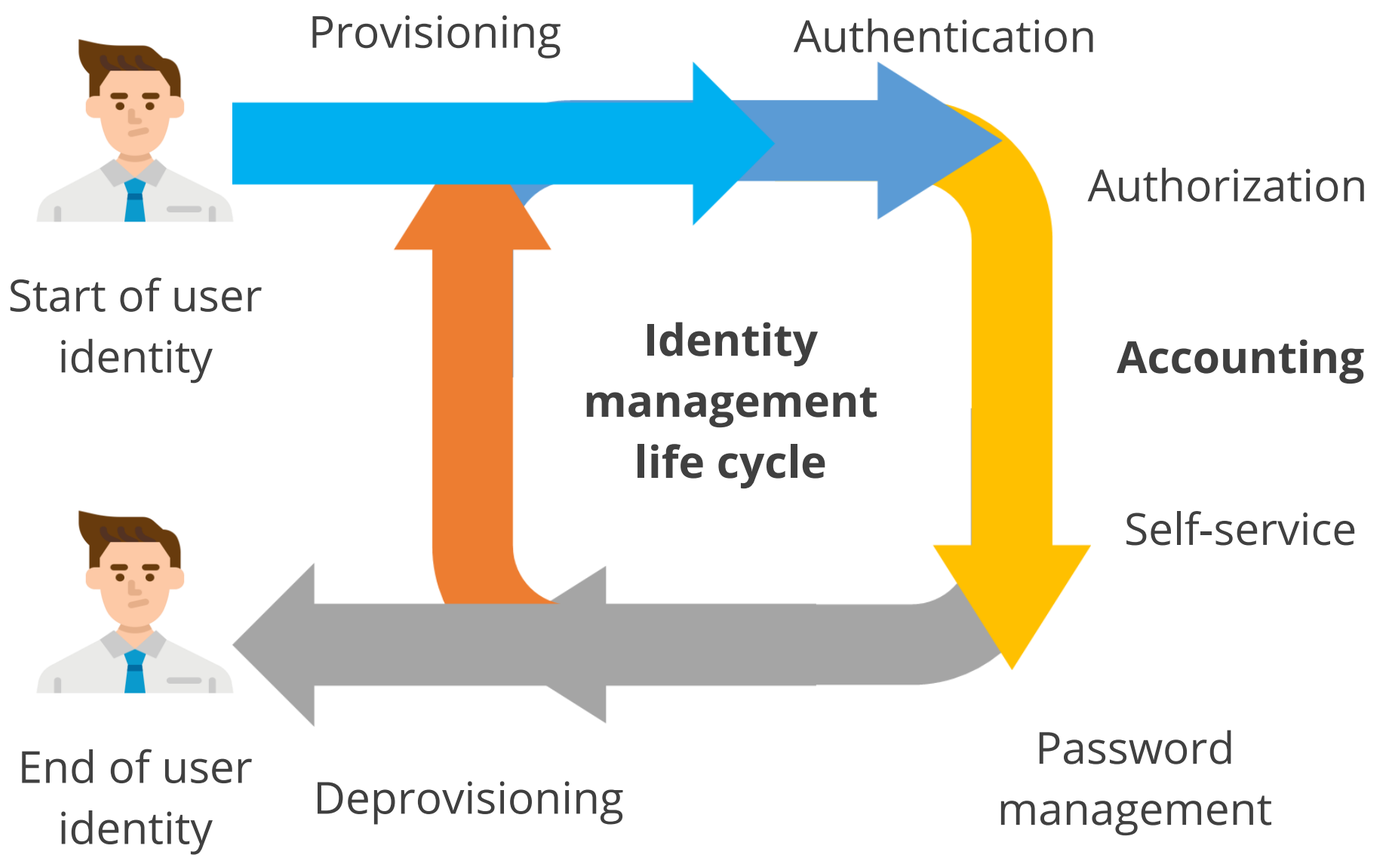
Identity Management Life Cycle



Authorization

Determine user’s rights to access the system

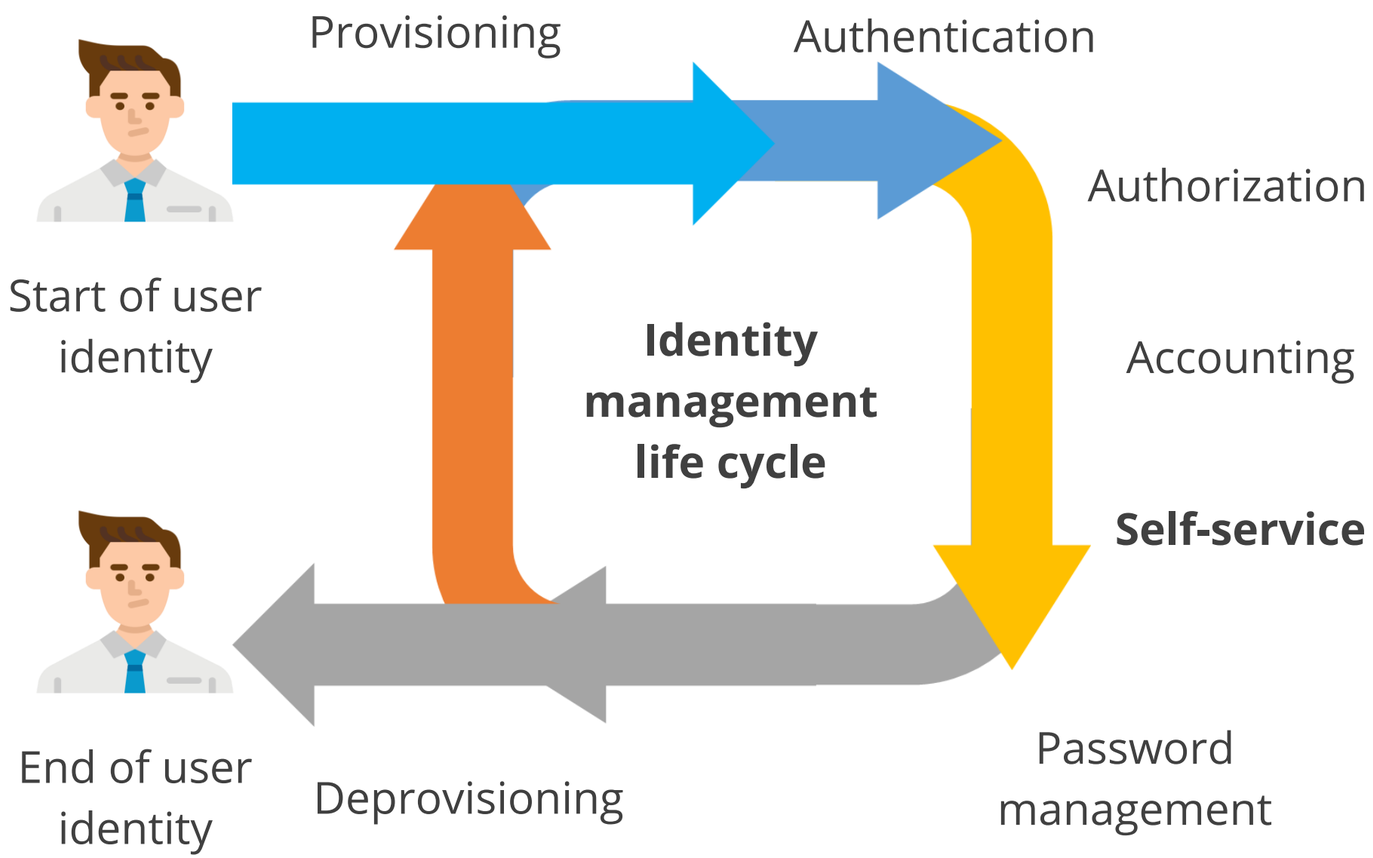
Identity Management Life Cycle



Accounting

- Record user's activities
- Implement non-repudiation
- Report audit and security issues

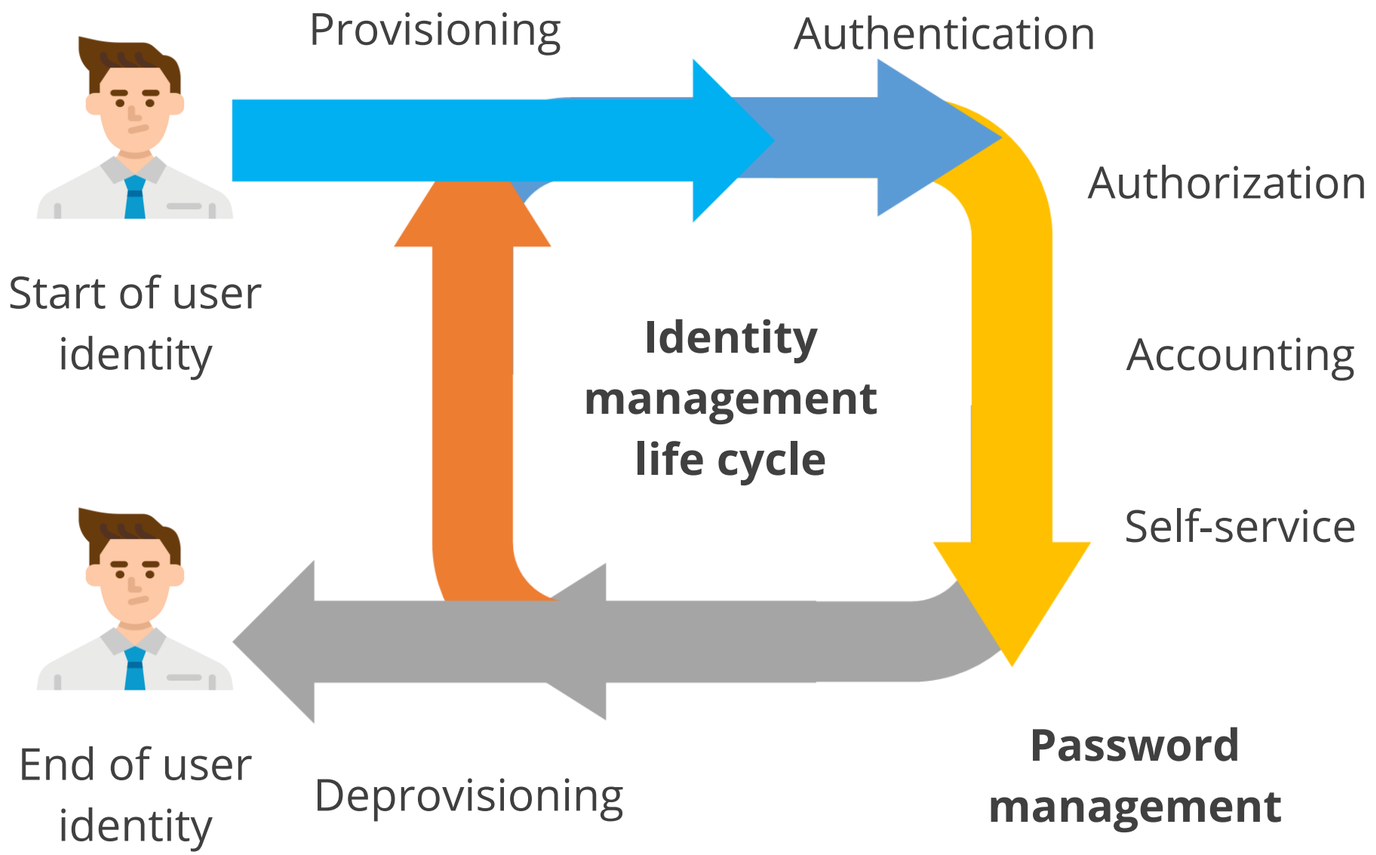
Identity Management Life Cycle



Self-service

- Change and reset passwords
- Update personal information
- Sync user attributes with other systems

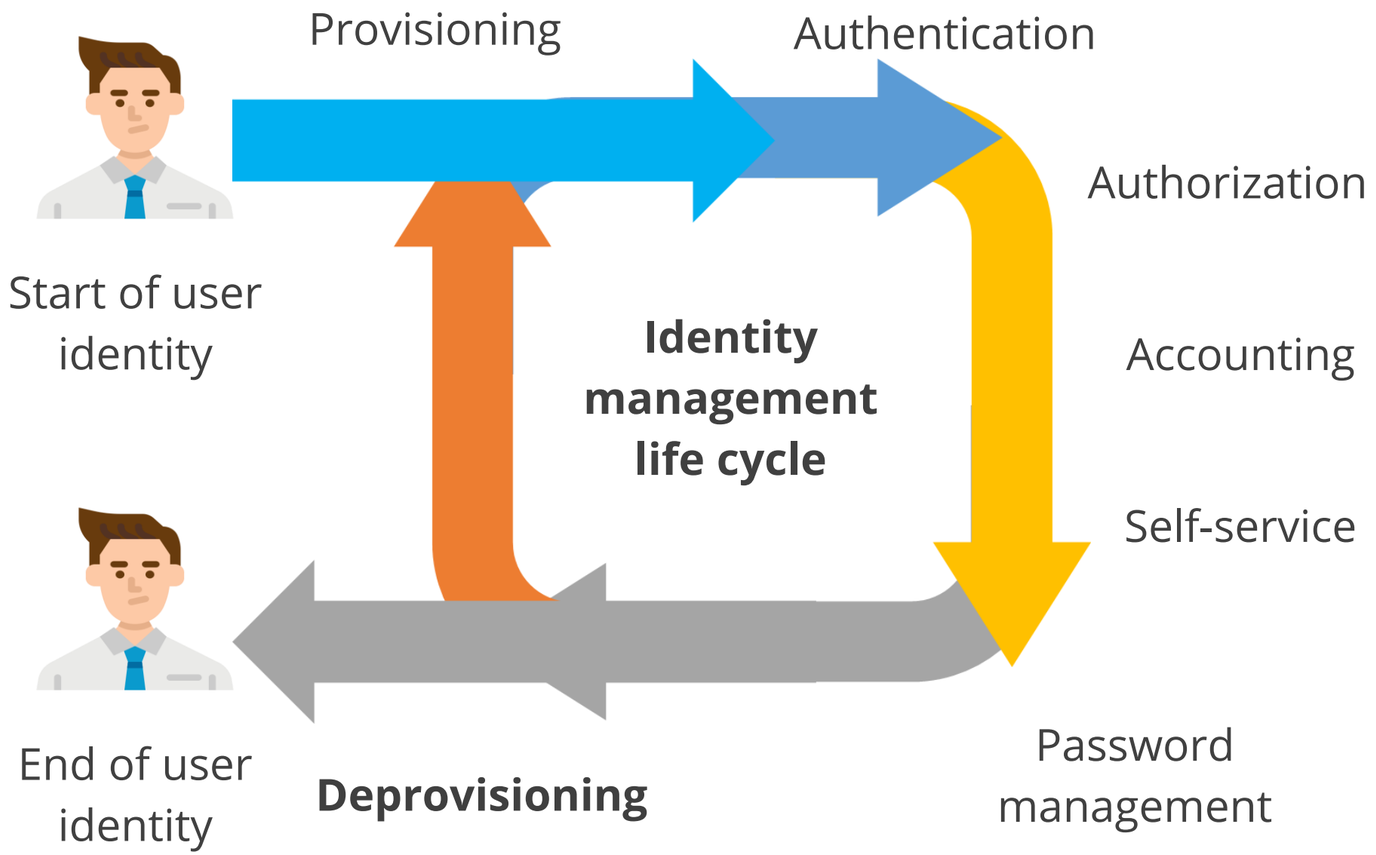
Identity Management Life Cycle



Password management

- Define password dictionary
- Enable password policy

Identity Management Life Cycle



Deprovisioning

- Revoke permissions and authorizations based on current roles
- Control security

Role Definition

A role is a set of one or more permissions that can be assigned to a user who inherits these permissions.

A permission allows users to perform actions on a resource.

A user can belong to one or more roles.

Roles and permissions should be assigned based on the principles of least privilege and need to know.

Account Access Review

This process is designed to review access rights periodically for all employees and vendors to identify excessive or escalating privileges.

- Creates service accounts specifically for use by services, applications, and virtual machines
- Grants elevated privileges and access to business-critical applications and data to service accounts
- Dictates policies to determine when accounts should be reviewed, deactivated, or deleted
- Conducts regular reviews or audits of service accounts to identify unusual behaviors that may indicate a breach or misuse

Privileged Accounts

They are user accounts with elevated permissions and access rights that allow them to perform tasks that ordinary users cannot.

- Includes highly privileged accounts like administrator (Windows) or root (Linux)
- Allows normal users to temporarily gain root privileges using the sudo command (Linux)
- Creates accounts specifically for services, applications, and virtual machines
- Assigns full administrative privileges without considering the principle of least privilege, posing a security risk if compromised

Privilege Escalation

Occurs when a malicious user gains higher levels of permissions, access, or privileges than they have been assigned

Happens due to administrative oversight, identity theft, or credential compromise

Horizontal Privilege Escalation

It occurs when an attacker gains rights and privileges of another user with similar privileges.

Attacker

Administrator

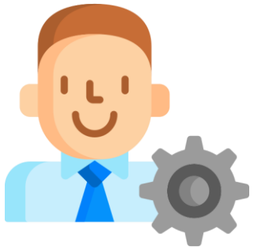
User

It is referred to as **account takeover.**

Vertical Privilege Escalation

It occurs when an attacker gains access to an account and tries to elevate its privileges.

Attacker



Administrator

User

It is also known as a privilege elevation attack, moving from low to high privileged access.

Privilege Escalation: Countermeasures

- Use multi-factor authentication
- Minimize the number and scope of the privileged accounts
- Follow the principle of least privilege

Privilege Escalation: Countermeasures

- Perform continuous monitoring of privileged accounts and keep a detailed logs of activities
- Analyze privileged accounts to identify and address risks, threats, sources, and attacker intents
- Prevent sharing of privileged accounts and credentials

Quick Check

You aim to prevent privilege escalation attacks in your organization. Which practice is most effective in preventing horizontal privilege escalation?

A. Multifactor authentication

B. Limiting permissions for groups and accounts

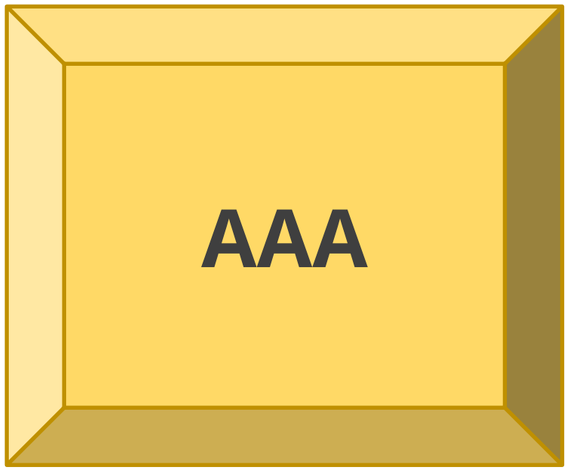
C. Disabling unused ports and services

D. Sanitizing user inputs to applications

AAA Protocols

AAA Protocol

It stands for authentication, authorization, and accounting and is a framework used to manage access and security in computer networks.

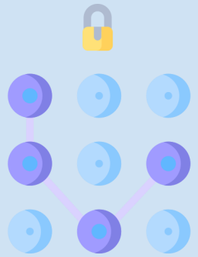


- It essentially regulates who can access network resources (authentication), what they're allowed to do once they're in (authorization), and tracks their activity (accounting).
- It is typically implemented on a centralized server, which can manage access control for multiple network devices.
- It simplifies administration and ensures consistent enforcement of security policies.

AAA Protocol

The following methods are used to achieve central authentication where every user is authenticated centrally.

RADIUS

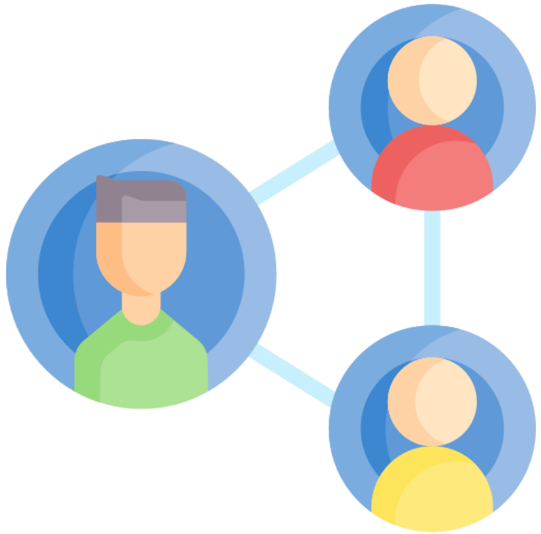


TACACS+

Diameter

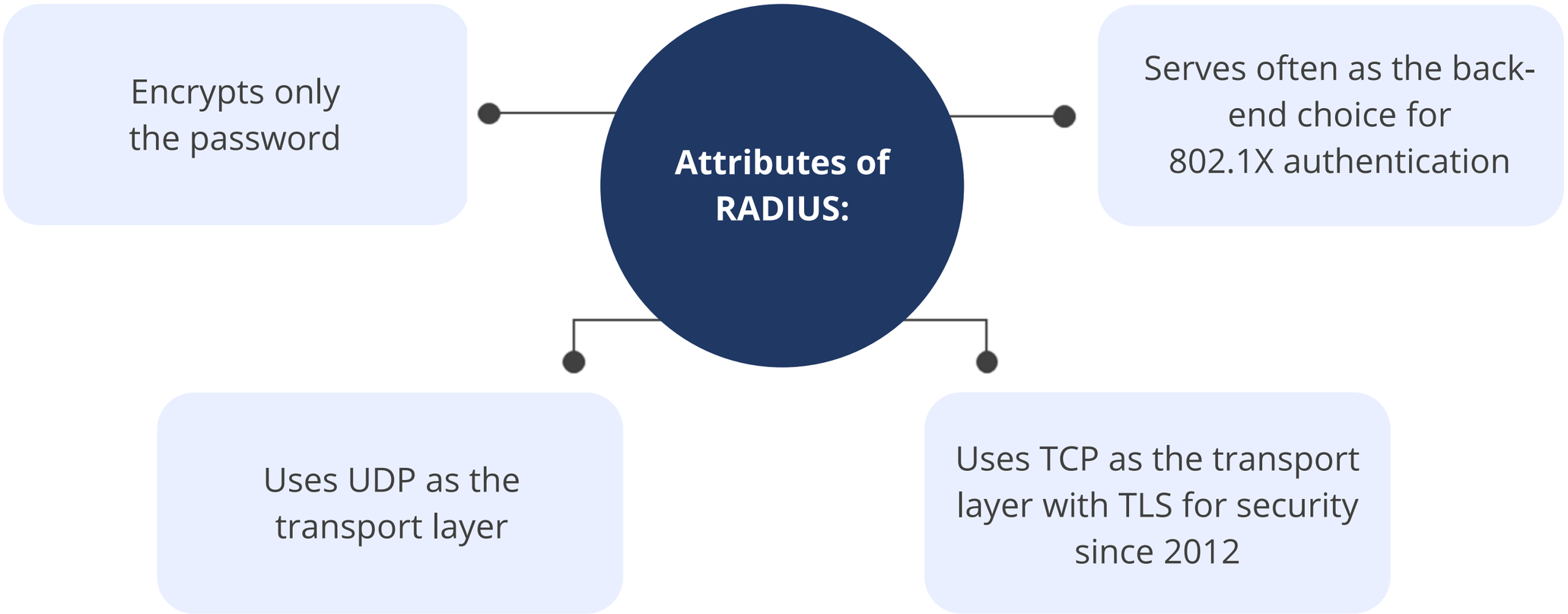
Remote Authentication Dial-in User Service (RADIUS)

It is a networking protocol created in 1991 to offer centralized authentication, authorization, and accounting (AAA) management for users that connect to and utilize a network service.

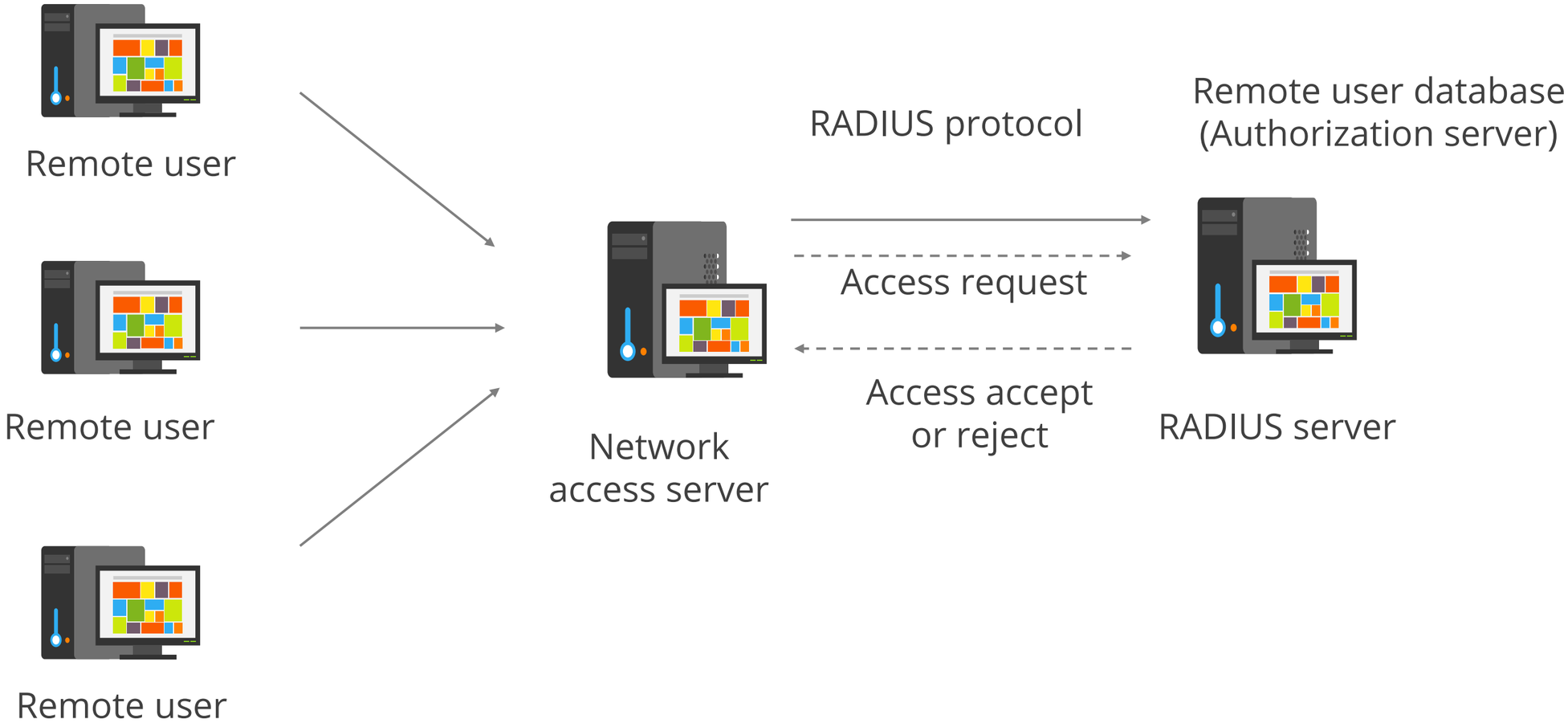


RADIUS: Attributes

It is a client or server protocol running in the application layer.



RADIUS: Working



Terminal Access Controller Access-Control System Plus (TACACS+)

It is a CISCO networking protocol that manages authentication, authorization, and accounting (AAA) through a centralized server.

Terminal Access Controller Access-Control System Plus (TACACS+)

It is a completely new protocol incompatible with TACACS and XTACACS.

It uses TCP to provide a high-quality connection.

It also encrypts packets sent and received from the TACACS+ server.

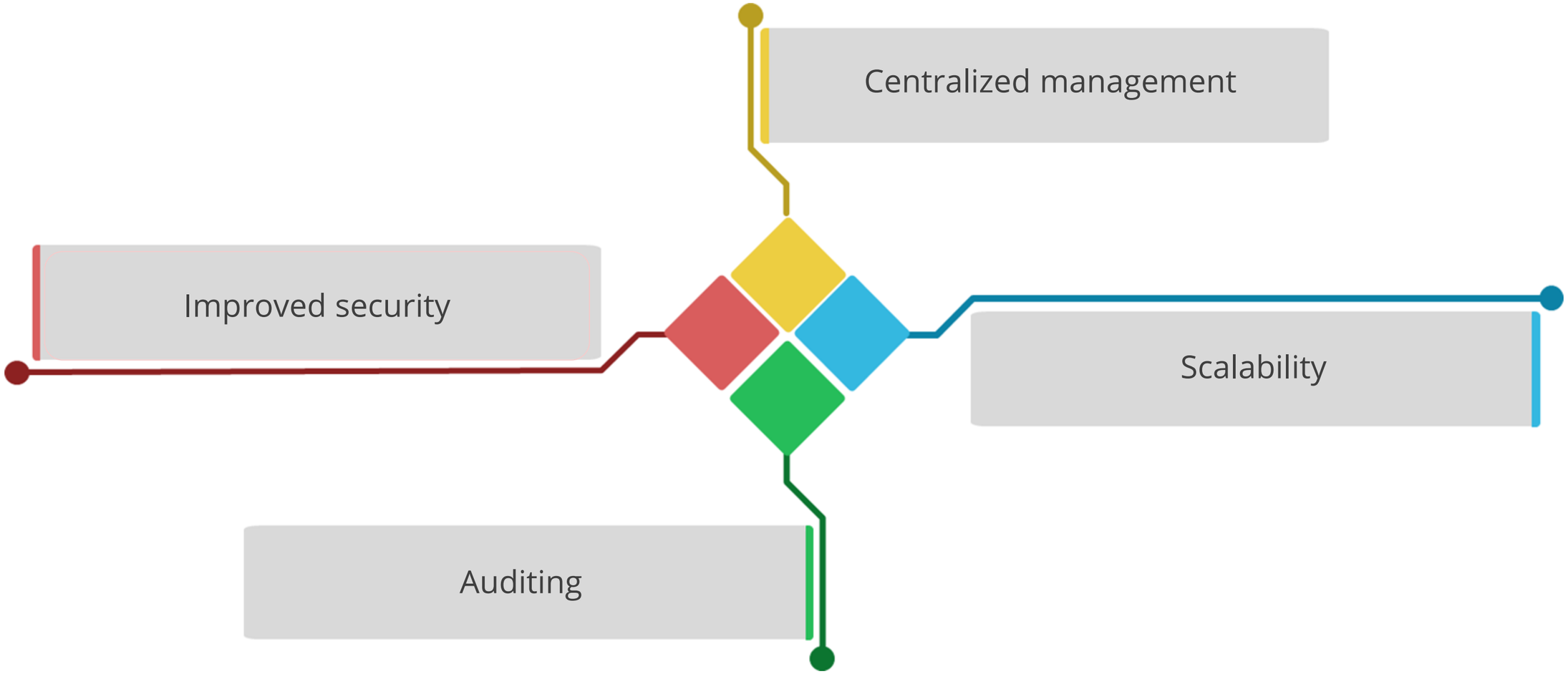
It separates the tasks of authentication, authorization, and accounting.

Diameter

It is a protocol that supports all forms of remote connectivity.

- It uses 32 bits for the attribute-value pair (AVP) field.
- It uses TCP port 3868.
- It uses existing encryption standards, including IPsec or TLS.
- It is a peer-based protocol.
- The server or client initiates communication.
- It has better error detection, correction, and failover functionality than RADIUS.

Benefits of AAA



Quick Check

You use a network sniffer to monitor traffic from RADIUS server configured with default settings. What protocol should be monitored, and what traffic would you be able to read?

A. TCP; none as all RADIUS traffic is encrypted

B. UDP; none as all RADIUS traffic is encrypted

C. TCP; all traffic except passwords which is encrypted

D. UDP; all traffic except passwords which is encrypted

Decentralized Access Control (DAC)

Decentralized Access Control (DAC)

It is a concept in cybersecurity that moves away from centralized control of access permissions.

- It provides access control decisions to people closer to the resources.
- It enables the functional manager to assign access control rights to employees.
- It allows changes to happen faster.
- It may lead to a conflict of interest.
- It does not provide uniformity and fairness across the organization.
- It can cause certain actions to overlap.

Decentralized Access Control (DAC)

In this approach, site administrators are responsible for managing their sites independently.
A sample scenario is as follows:

Site D

Site C

Site A

Site B

Access Control Best practices

- Deny access to systems for undefined users or anonymous accounts
- Limit and monitor the use of administrator and other powerful accounts
- Suspend or delay access capability after a specific number of unsuccessful logon attempts
- Remove obsolete user accounts as soon as users leave the company
- Enforce strict access criteria
- Enforce need-to-know and least-privilege practices

Access Control Best practices

- Suspend inactive accounts after 30 to 60 days
- Disable unnecessary system features, services, and ports
- Replace default password settings on accounts
- Remove redundant IDs, accounts, and role-based accounts from resource access lists
- Enforce strong password requirements
- Ensure that if the same message is encrypted with the same key and sent twice, its ciphertext is the same

Key Takeaways

- Access controls protect systems and resources from unauthorized access.
- Identity management is the use of different products to identify, authenticate, and authorize users through automated means.
- Multifactor authentication is a type of authentication that necessitates the use of more than one authentication factor to be successful.
- The two types of access control administrations are centralized and decentralized.
- AAA is used to manage access and security in computer networks and stands for authentication, authorization, and accounting.

Thank You