# Certified Information Systems Security Professional (CISSP) Certification Training Course

# 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
- Manage identification and authentication of people, devices, and services
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle and implement authentication systems

# Introduction to Identity and Access Management

# Importance of Identity and Access Management in Information Security


Kevin received an email from Sergei Stankevich, the project manager of the firewall division. The email stated that, as a part of the strong focus on security that financial year, Nutri Worldwide Inc. would perform two cycles of security audits instead of one. The following processes would be audited during the year:

- Access Controls
- Access Control Implementation
- Access Control Monitoring

# Importance of Identity and Access Management in Information Security

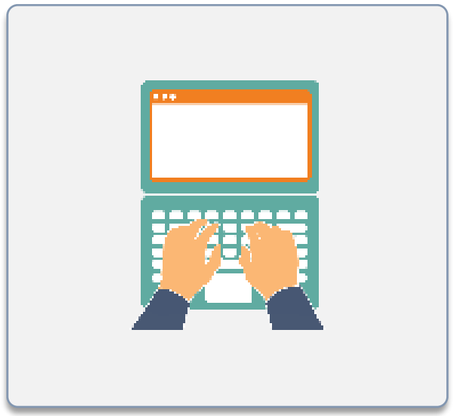
**Mission Statement:**

Protecting networks, applications, and data from attack is of utmost importance. This will be achieved by:

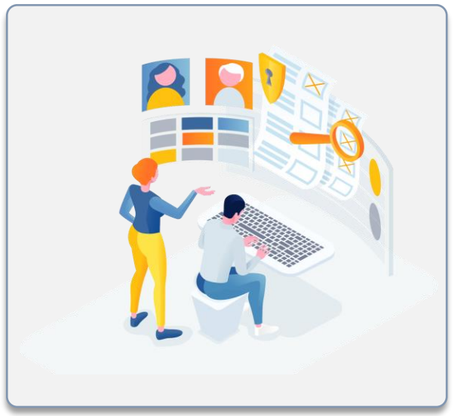
- Auditing current security practices, policies, and processes to suggest improvement actions to be implemented
- Examining and authenticating security through penetration testing and vulnerability assessments

# Access, Subject, Object, and Access Controls

The terms access, subject, object, and access controls are defined below.

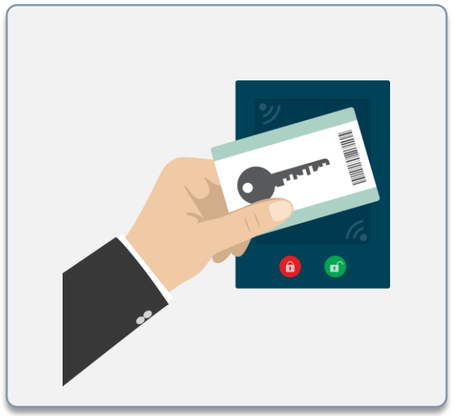


Access is the transfer of data between subjects and objects.



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 how a user or system interacts and communicates with other systems and resources.

# Control Physical and Logical Access to Assets

# Controlling Access to Assets

| | |
|---|---|
| **Information** | Threats to information include loss of data confidentiality, integrity, and availability. Access control must be implemented to prevent unauthorized access to the information. |
| **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 such as laptops, desktops, servers, tablets, and smartphones must be restricted. As more organizations adopt bring your own device (BYOD) policies, they need to protect these devices. Using mobile device management (MDM) becomes important. |
| **Facilities** | Organization's facilities must be protected by implementing policies and procedures to limit physical access to only authorized personnel. Employee access to restricted business locations and proprietary areas, such as data centers must be controlled, tracked and audited. |
| **Applications** | Application access controls are used for managing user authentication and implementing rules that determine user access to applications and data. |

# Manage Identification and Authentication of People, Devices, and Services

# Identity and Access Management Policy

The first element of an effective access control program in an organization is to establish identity and access management policy and related standards and procedures.

# Identity and Access Management Policy

The identity and access management policy:

Specifies the way users and programs are granted access through proper identification and authentication

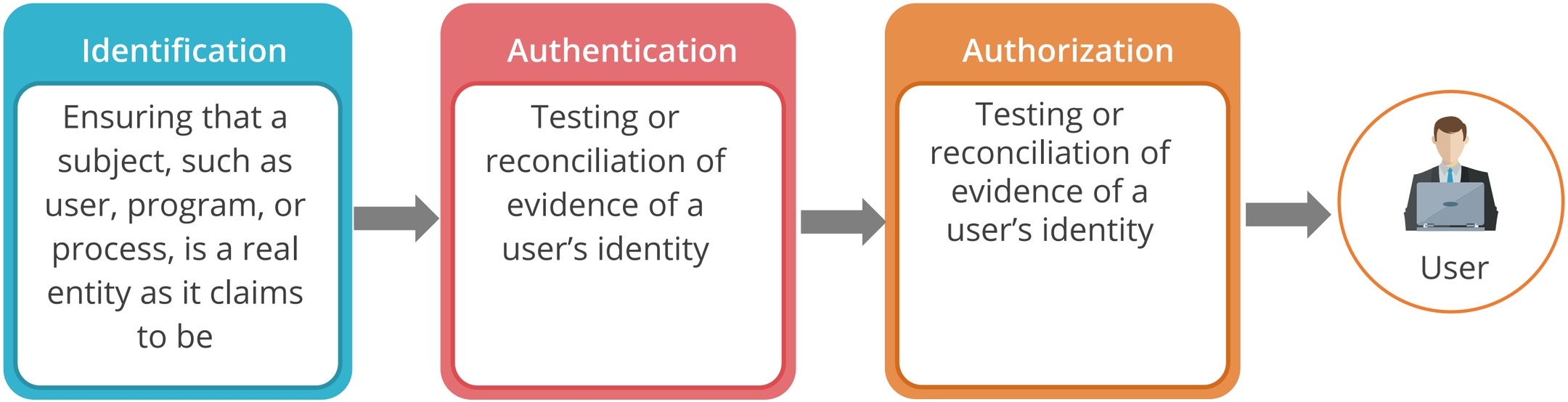

Specifies the guidelines of granting privileges to various resources

Improves the governance process

Prevents inconsistencies in provisioning, administration, and access control management

# Identification, Authentication, and Authorization

To be able to access a set of data or a resource, a subject has to be identified, authenticated, and authorized. The process is shown below:



# Identity Management

It describes the management of individual identities, their authentication, authorization, and privileges or permissions within or across the system and enterprise boundaries.

Identity management is the use of different products to identify, authenticate, and authorize the users through automated means.


The goal is to increase the security and productivity while decreasing the cost, downtime, and repetitive tasks.

# Identification Methods

To ensure that an application is authorized to make requests to potentially sensitive resources, the system can use digital identification, such as a certificate or one-time session.

**Some of the most common types of identification methods are as follows:**

- 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

- The user identification must be unique.

## Non-descriptiveness

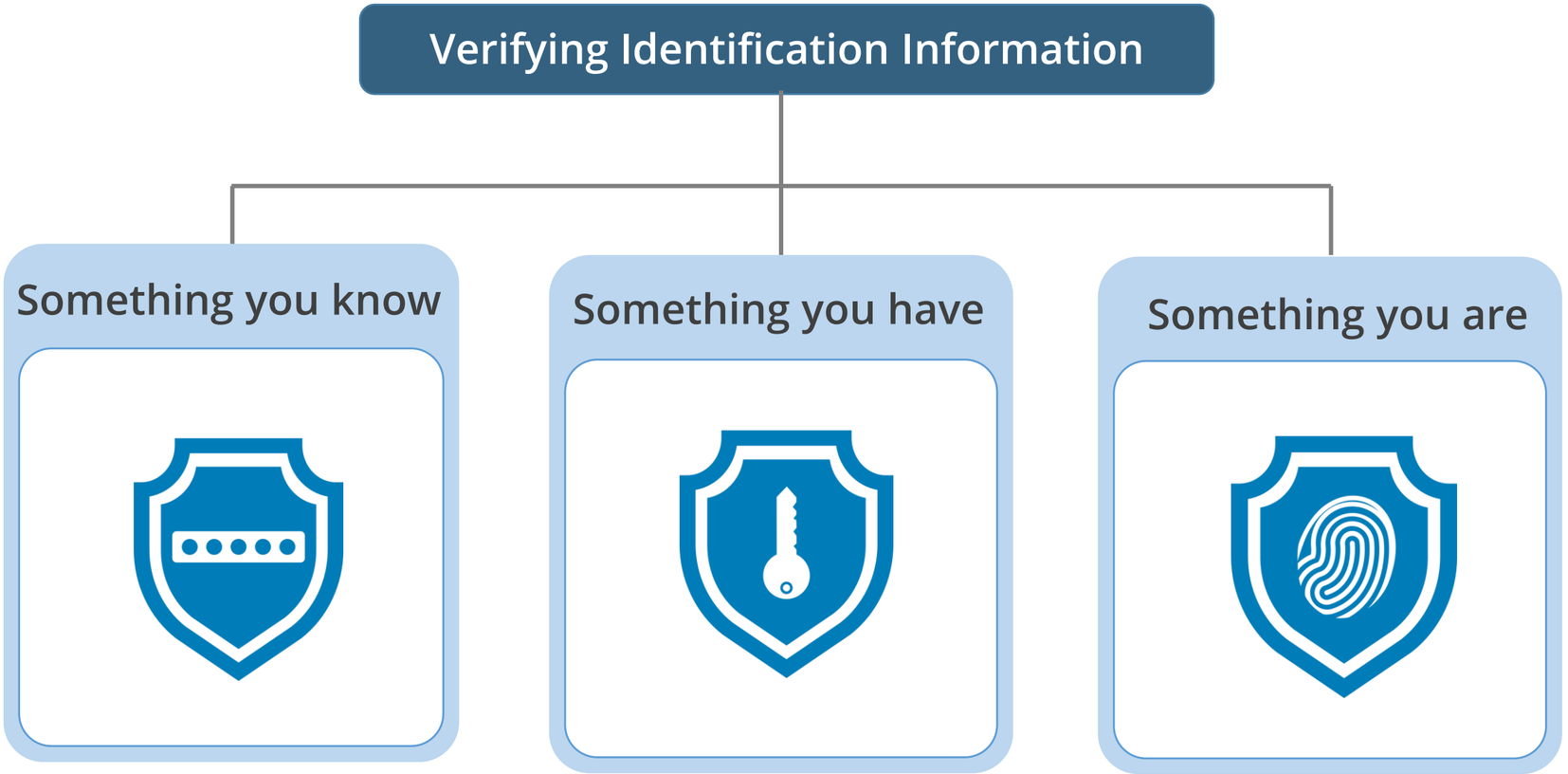
- The user's role or job function should not be exposed by Identity (ID).

## Secure issuance

- ID issuing process must be well documented and secure.

# Verifying Identification Information

- The function of identification is to map a known quantity to an unknown entity to make it known.
- There are three general factors that can be used for verifying identification.

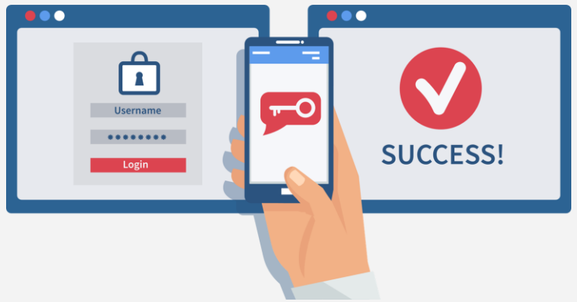


# Multi-Factor Authentication

Depending on the number of factors used, there are two ways of strengthening the authentication.

## Two-Factor Authentication

A secure method of authentication in which the user is required to provide at least two out of the three identification factors




## Three-Factor Authentication

The highest level of security where the user is asked to provide all the three identification factors

# Biometrics: Characteristics

Biometrics, based on individuals' physiological and behavioral characteristics, is one of the most effective and accurate methods of verifying identification.

## Acceptance

- Refers to user acceptance of biometric system
- Depends on privacy intrusiveness and psychological or physical discomfort

## Throughput Rate

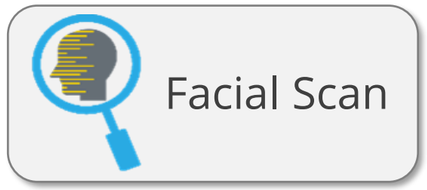
- Also called biometric system response time
- Refers to the time taken to process the authentication request

## Enrollment Time

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

# Types of Biometrics

Biometrics commonly used for identification:


Facial Scan


Fingerprint


Hand Geometry


Iris Scan


Signature


Keyboard Dynamics


Voice Print


Retina Scan

# Discussion

# Discussion

A retina scan is a biometric technique that uses the unique patterns on a person's retina blood vessels to identify them.

Even though the retina scan is considered to be one of the most accurate biometric systems, why is it not preferred by most organizations?

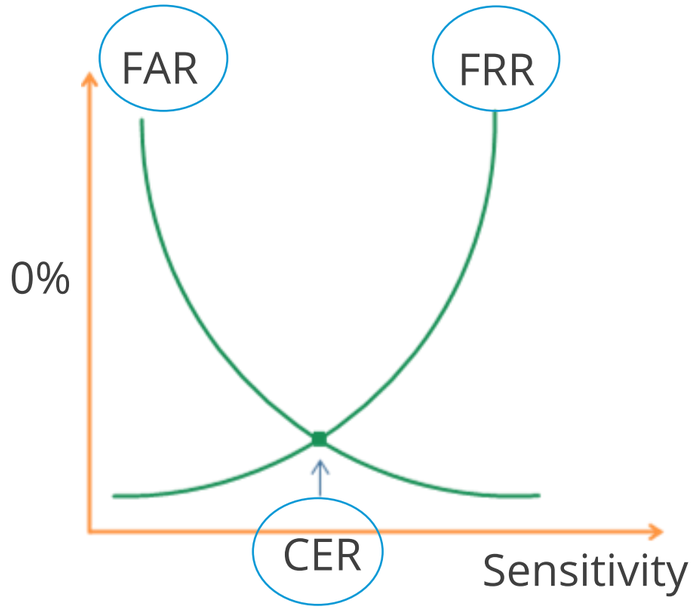
# FRR, FAR, and CER

To measure the accuracy of a biometric system, the following are used:

**False Rejection Rate (FRR):** The biometric system rejects an authorized individual.

**False Acceptance Rate (FAR) or Type II error:** An impostor who should be rejected is accepted by the system.

**Crossover Error Rate (CER):** When the false acceptance rate equals the false rejection rate, that point represents CER. The lower the value of CER, higher the accuracy of the biometric system. For example, a system with a CER of 3 has greater accuracy than a system with a CER of 4. CER is also known as Equal Error Rate (EER).



# Passwords

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

## Problems with Passwords

- Insecure
- Easily broken
- Inconvenient
- Repudiable

## Common Password Attacks

- Dictionary (Crack, John the Ripper)
- Brute force (Lophtcrack)
- Hybrid attack (Dictionary and Brute Force)
- Trojan horse login program (Password sending Trojans)
- Social engineering

# Password Types

Different types of passwords are described below:

**Passphrase**

Longer than a password, in the form of a sequence of characters

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

**Cognitive Passwords**

Individual's identity is verified 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)**

Dynamic password will be valid for only one login session or transaction.

- OTP a bank sends to a customer via SMS

# Password-Based Attacks

**Electronic monitoring (replay attack):**
- Listening to network traffic to capture authentication information

**Access to the password file:**
- Usually done on the authentication server
- Capturing the file will give access to the passwords of many users

**Brute-force attack:**
- Performed through automated tools that cycle possible combinations on the password dump

**Dictionary attack:**
- Comparing thousands of dictionary words to a users' password for a successful match

**Social engineering**:
- Falsely convincing an individual to share authentication information

**Rainbow table:**
- Using a table that contains all possible passwords in a hash format

# Tokens

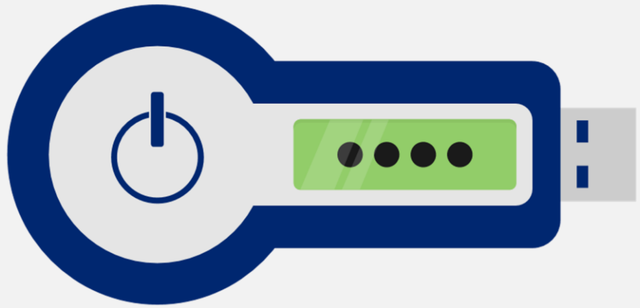
**Tokens are used to prove the identity of a user and authenticate the user to a system or an application.**

- They can be software based or hardware based.
- An attacker can compromise the security by gaining control of the token and impersonating the token owner. This may also compromise the authentication protocol.
- Tokens must be secured, as they may be cloned, damaged, lost, or stolen from the owner.

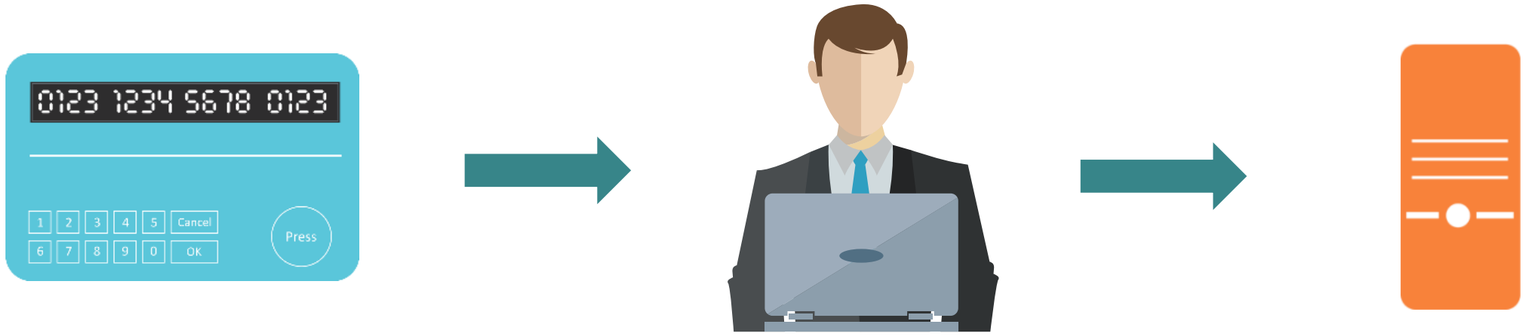
# Token Device: Synchronous

**Time based:**

- This requires synchronized internal clocks between the token device and the authentication server.
- The secret key and time on token are used to generate one-time password.
- RSA token is an example of time-based synchronous token.



# Token Device: Synchronous

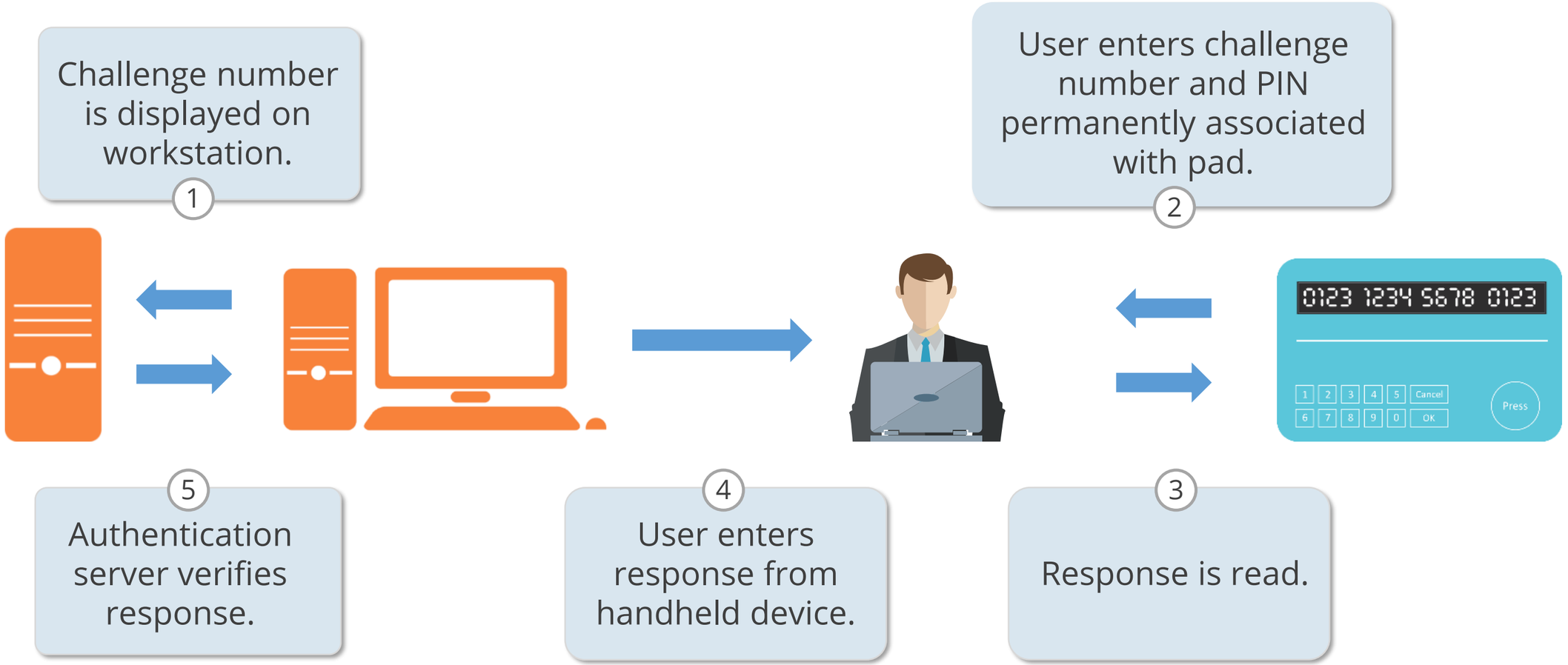



1. Every minute clock reading is enciphered with a secret key and displayed. This is one-time password.
2. User reads secret key and enters the data into workstation along with the PIN.
3. Authentication Server knows secret keys to all cards by clock synchronization with the cards. It verifies the entered data.

# Token Device: Asynchronous

Challenge-response is used to authenticate a user.

**Example: Grid Cards.**



# Authorization Concepts

Authorization is based mainly on the following concepts.

**Need-to-know principle** → According to this principle, the subject is given access to specific information depending on the subject's job, duties, and requirements.

**Authorization creep** → This occurs when an employee who works for an organization moves from one department to another and is assigned new access rights and permissions without the old permissions being reviewed and removed.

**Access control list (ACL)** → It specifies the subjects who are granted access and the operations allowed on objects.

**Default to zer** → Access controls should always start with zero access. The administrator can then allow various accesses based on the organization's security policy.

# Accountability

Accountability helps hold users responsible for their own actions and ensures proper enforcement of security policies. The following gives a broad overview of the items and actions that can be audited and logged:

## System-level events

- System or computer performance
- Successful and unsuccessful login attempts
- Timestamps of the login attempts

## Application-level events

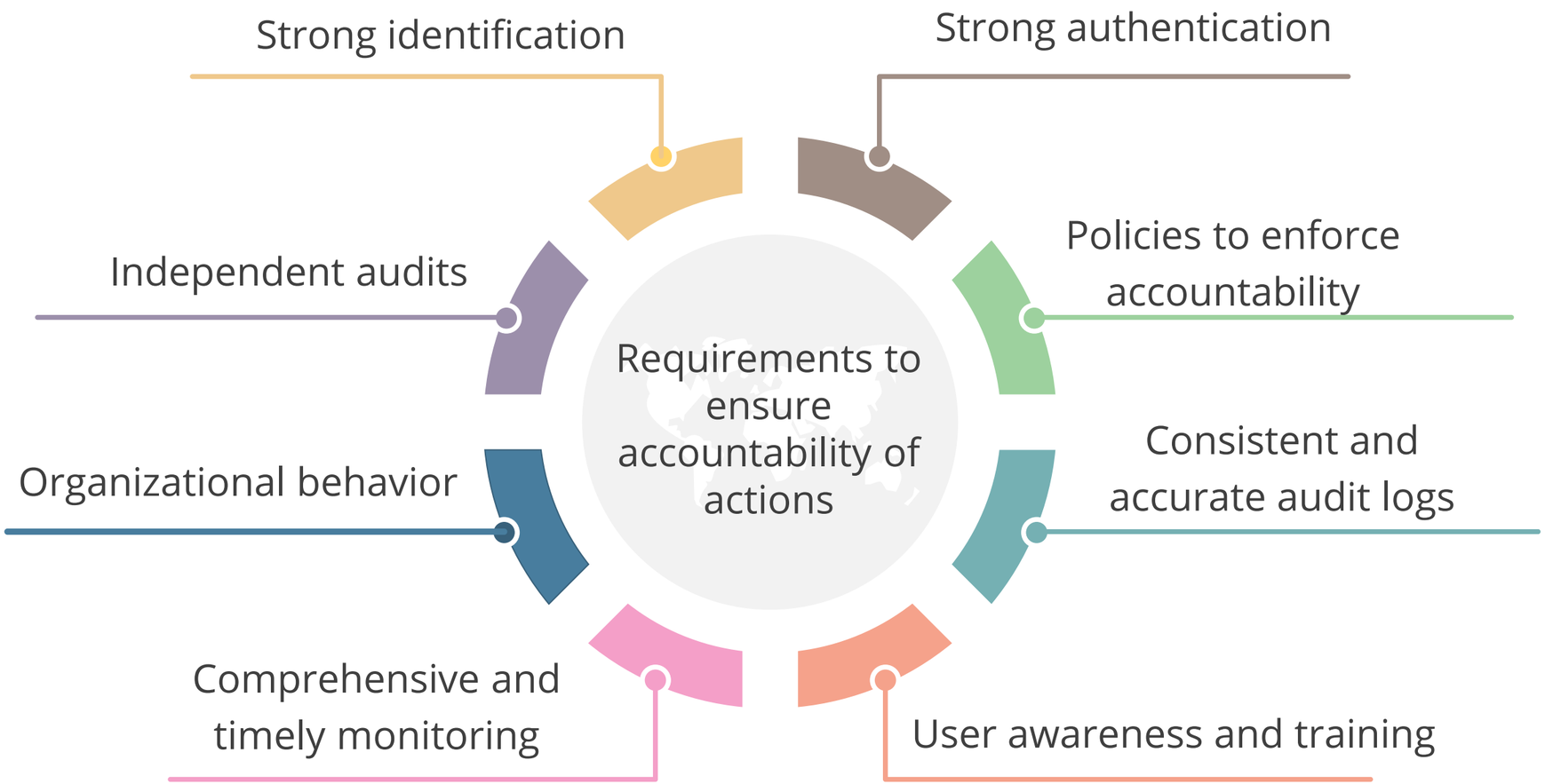
- Error messages
- File modifications

## User-level events

- Identification and authentication attempts
- Commands used

# Accountability

Non-repudiation plays an important role in accountability to ensure that users, processes, and actions are responsible for impacts.



# Session Management

Session is the term used to describe a single entity communicating with another for a specified period of time. The way a single instance of identification, authentication, and authorization is applied to the entities is termed **session management**.

**Control and protection of desktop sessions can be achieved through:**

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

# Registration, Proofing, and Establishment of Identity

Identity proofing is the process of establishing a reliable relationship electronically between the individual and the credential for electronic authentication purposes.

**This is done by collecting and verifying information to prove that the person who has requested a credential, an account, or other special privileges is indeed who they claim to be.**

- It involves in-person evaluation of a driver's license, birth certificate, passport, or any other identity issued by the government.
- Certification and accreditation should be carried out for the process of identity proofing and registration.

# Federated Identity Management (FIM)

## Federated identity

- It is a portable identity, and it along with its associated entitlements can be used across business boundaries.
- It allows a user to be authenticated across multiple IT systems and enterprises.
- Identity federation is based upon linking a user's otherwise distinct identity at two or more locations without the need to synchronize or consolidate directory information.

# Federated Identity Management (FIM)

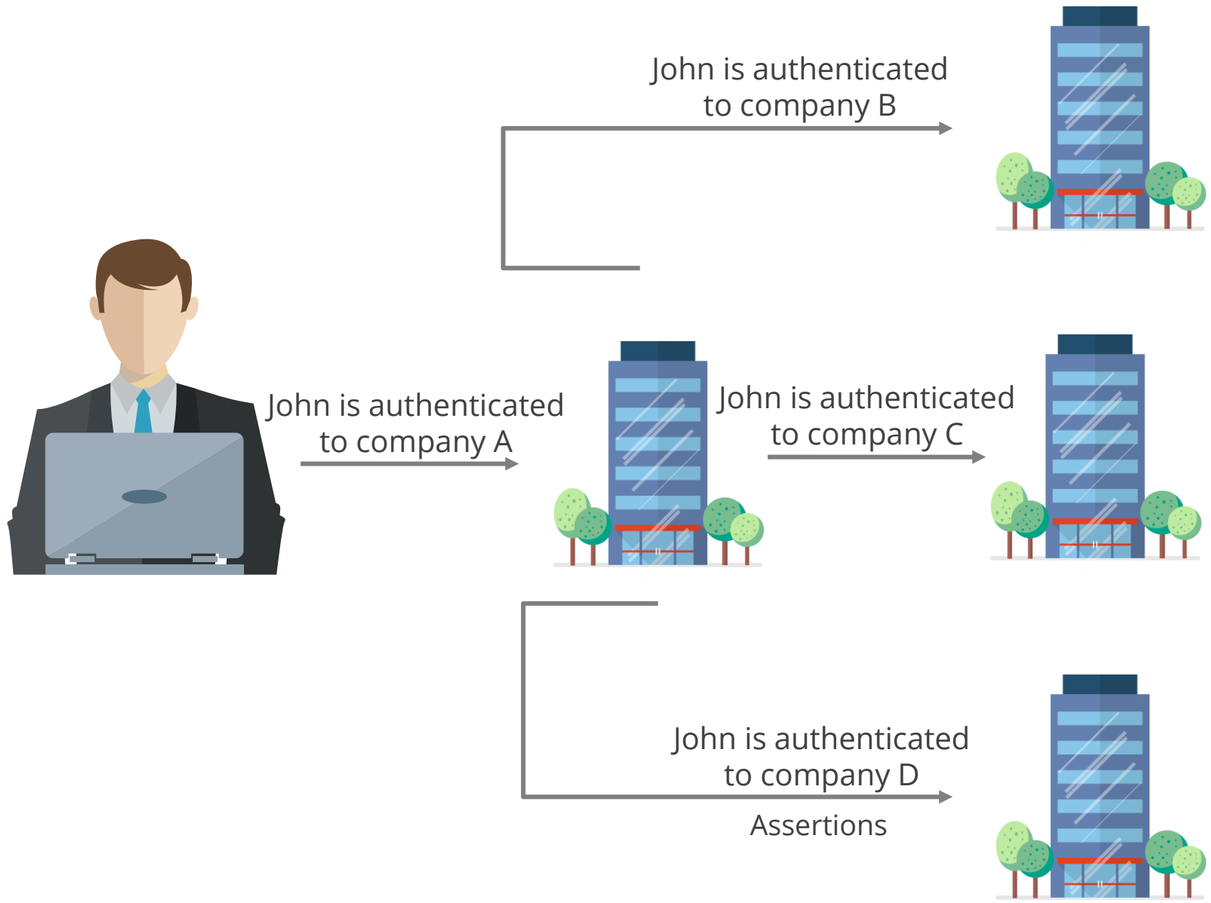
## Federated identity management

- Federated identity management addresses the identity management issues that arise when multiple organizations need to share the same applications and users between them.
- In a federated environment, each organization in the federation subscribes to a common set of policies, standards, and procedures for the provisioning and management of user identification, authentication, and authorization information.
- A trust relationship is established among participating organizations.

# Federated Identity Management (FIM): Example

When you book a flight on Expedia, the website asks if you also want to book a hotel room. If you click Yes, you could then be brought to the Taj Hotel website, which provides information on the hotel closest to the airport you are flying into.

You don’t have to log in again to book a room. You logged in on the Southwest website, and that website sent your information over to the Hilton website, all of which happened transparently.



# Credential Management Systems

A security practitioner can build a good Credential Management System by incorporating the following:

- Password history
- Strong passwords
- Fast password retrieving
- Generating passwords effortlessly
- Well-defined access control
- Controlling credentials
- Failover and redundancy
- Safely keeping passwords
- Preparedness for disasters
- Tracking and auditing access

# 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

- High level of assurance
- Meets the required security standards
- Simplifies compliance, administration, and auditing

# Single Sign-On (SSO)

In single sign-on (SSO), the user needs to enter credentials only once to get access to all the corporate resources that are entitled to the user.

| Pros | Cons |
| --- | --- |
| The user has one password for all enterprise systems and applications | Difficult to implement |
| Only one strong password needs to be remembered and used | Centralized point of failure |
| The user accounts can be easily created on hire and modified and deleted on dismissal | Compromises data |

# Difference Between FIM and SSO

## Federated identity management (FIM)

- FIM enables a single credential to access multiple applications and resources across multiple organizations.
- FIM gives you SSO.

## Single sign-on (SSO)

- SSO enables a single credential to access multiple applications and resources within one organization.
- SSO doesn't necessarily give you FIM.

# Just-In-Time (JIT)

Just-in-time (JIT) enables organizations to grant users on-demand and privileged access to applications or systems for a predetermined period of time on an as-needed basis.

These time-restricted accesses can be automated so that users don't have to wait for human approval.

The requests can be verified against a pre-approval policy or can be reviewed by an administrator who has the power to grant or deny the requests for short-term privileged access.

JIT access can be provided using ephemeral certificates which is a type of limited access security token that is automatically created on-demand, automatically expires, and requires no installation, configuration, or updation.

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

Information source: www.centrify.com/pam/privilege-elevation/time-based-role-assignment/

# Business Scenario

Kevin was concerned about the security of the cloud virtual machines and wanted to reduce the risk of privileged access abuse and lateral movement by threat actors.

He learnt about the just-in-time (JIT) access, which enables always-on access by enforcing time-based restrictions based on behavioral and contextual parameters.

After he enabled the JIT feature on the VMs, he created a policy which can determine the ports to be protected, how long ports remain open, and the approved IP addresses from where these ports can be accessed.

He enabled just-in-time access to lock down the virtual machines at the network level by blocking inbound traffic to management ports such as 22 (SSH) and 3389 (RDP).

The JIT access allowed Kevin to control the access and reduce the attack surface to his virtual machines by allowing need-based access for a limited period of time.

# Federated Identity with a Third-Party Service

# Identity as a Service (IDaaS)

**Identity as a a service (IDaaS)** is an SaaS-based **IAM** solution built and operated by a third-party provider. An IDaaS is provided as a subscription-based service**.**

**The key features of IDaaS are:**

### User management and access control

IDaaS provides administrative tools for onboarding users and managing their access privileges throughout the course of their employment.

### Multi-factor authentication (MFA)

Users are required to submit multiple factors to gain access to their resources thus providing greater security than single-factor authentication (username and password).

### Single Sign-On (SSO)

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

# Federated Identity

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

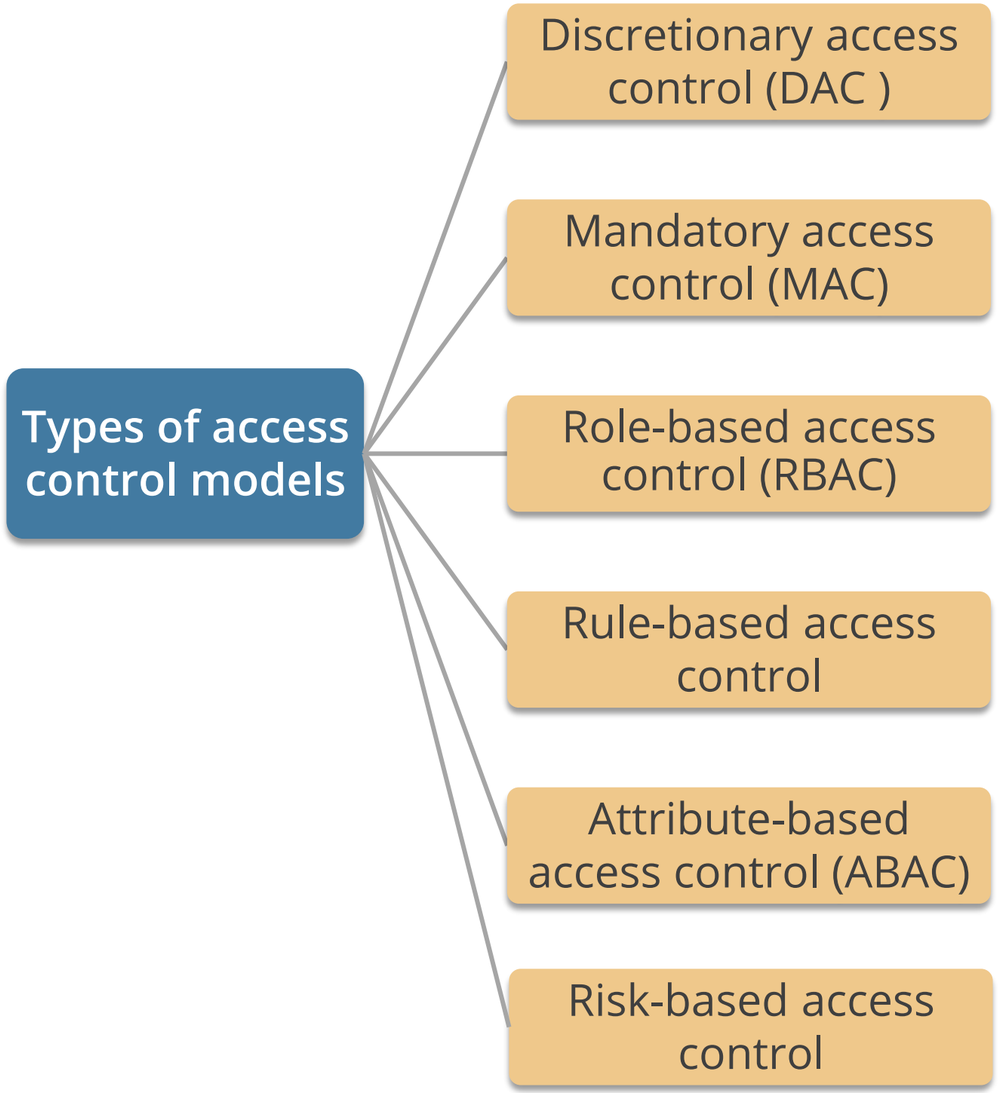
A unified identity management system minimizes administrative effort in managing accounts and controlling access and provides a single end-user authentication process across a hybrid environment.

# Implement and Manage Authorization Mechanisms

# Access Control Models

## Access control models

- An access control model is a framework that dictates how subjects access objects.
- Each model type uses different methods to control how subjects access objects, and each has its own merits and demerits.
- The business and security goals of an organization will help prescribe what access control model it should use.
- These models are built into the core or the kernel of the different operating systems and possibly their supporting applications as well.

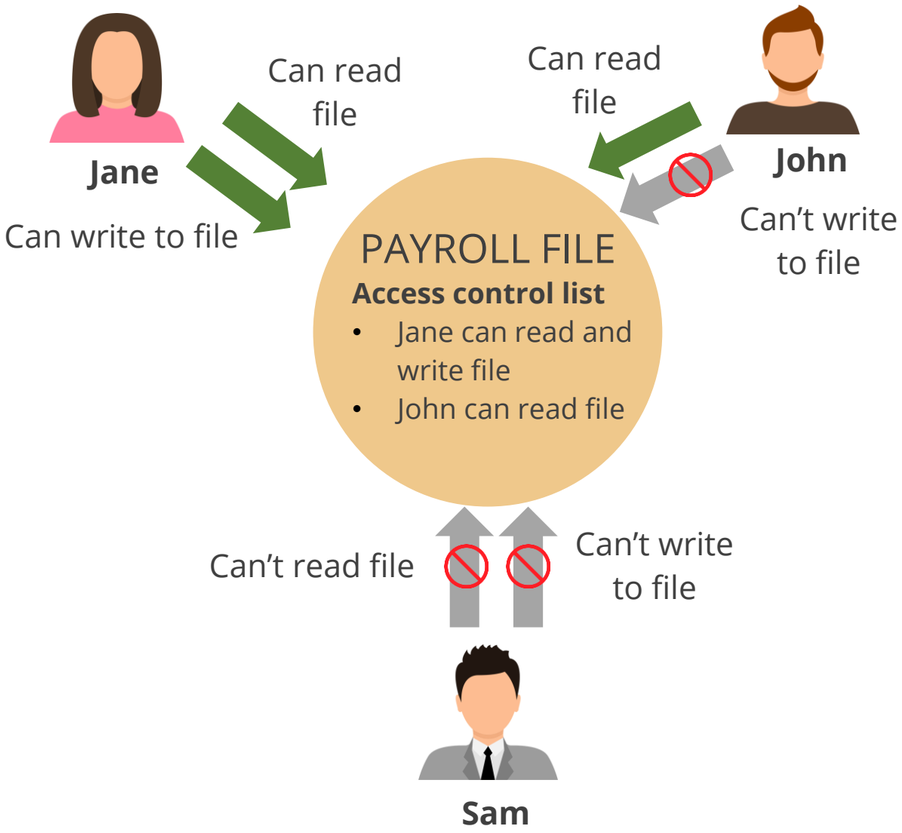


# Discretionary Access Control (DAC)

The way in which a subject will access an object is guided by an access control model. A model must be chosen to fulfill the directives of the security policy.

## DAC model

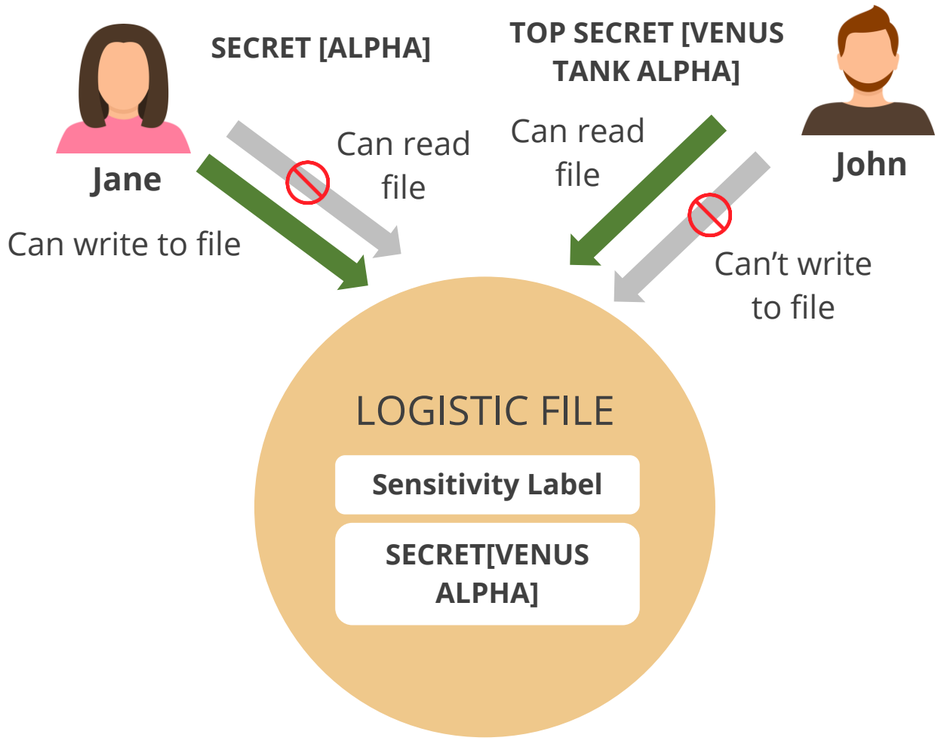
- Access to resources will be decided by data owners.
- The access control depends on the owner's discretion and authorization granted to the users.
- Access control lists (ACLs) are used to enforce the security policy.



# Mandatory Access Control (MAC)

## MAC model

- System's security policy is enforced by the operating system with the use of security labels.
- The resources have security labels that contain data classification, and the users have security clearances.
- When information classification and confidentiality is important, this model is used.



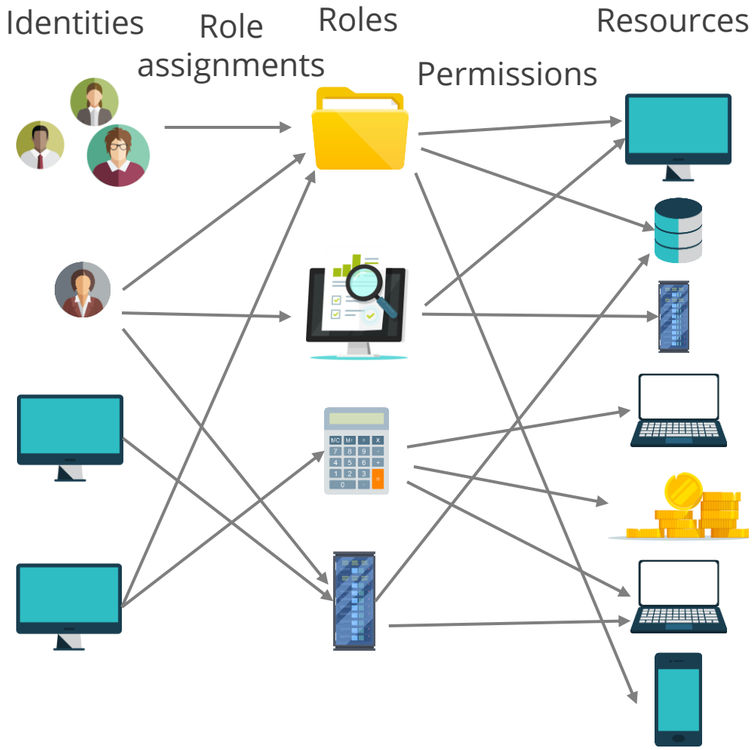
# Role-Based Access Control (RBAC)

Also known as nondiscretionary access control, access here is granted depending on the subject's role and designation.

## RBAC model

Four commonly used RBAC architectures:

- Non-RBAC
- Limited RBAC
- Hybrid RBAC
- Full RBAC



# Rule-Based Access Control

Access requests are evaluated against a specified list of predefined rules that determine what access should be granted.

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

They are not necessarily identity-based, that is, they can be applicable to all the users or subjects irrespective of their identities.

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

# Attribute-Based Access Control (ABAC)

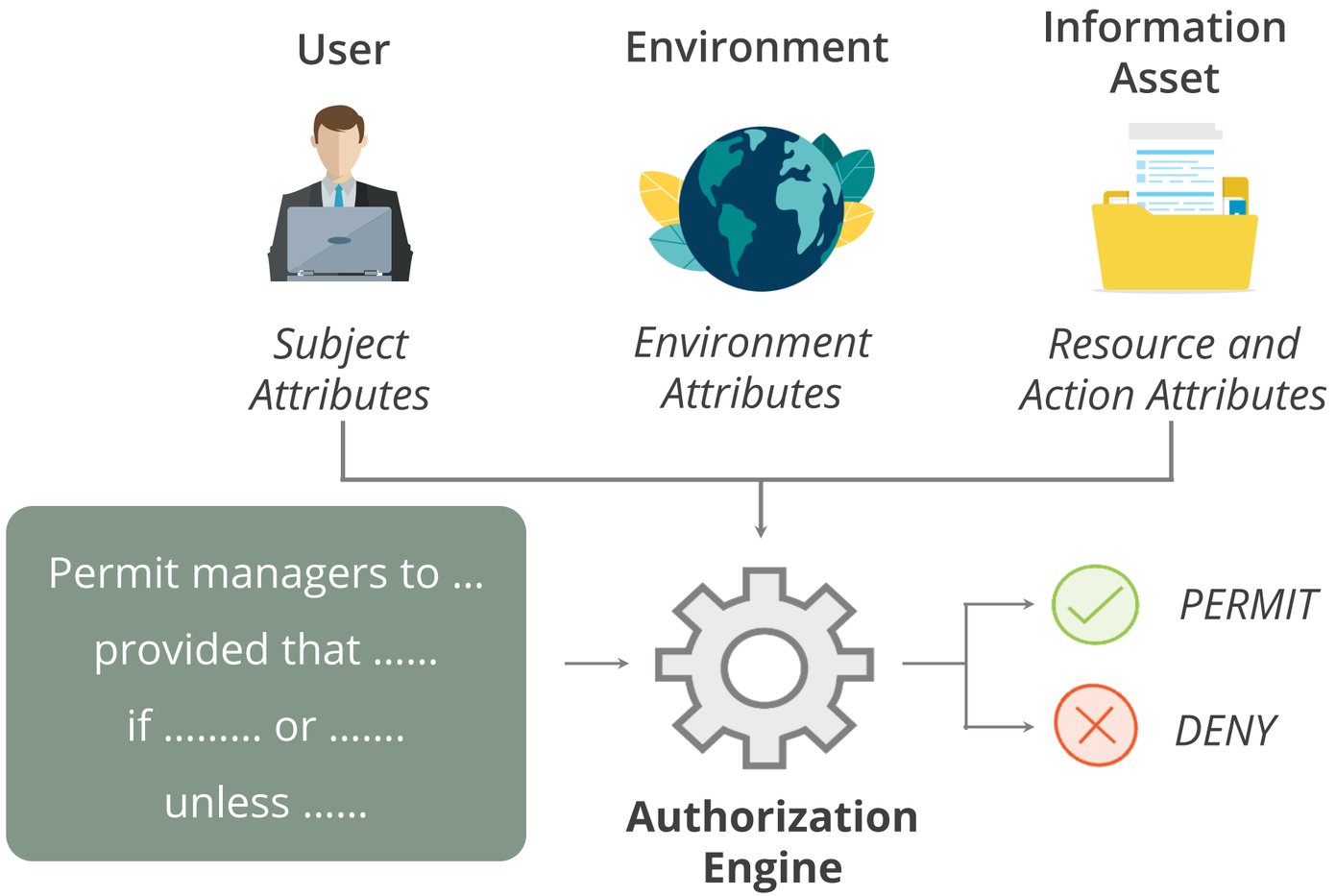
"An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions."
~ NIST

Granular policies can be established based on a combination of these attributes to grant or deny access.


Attributes provide details for building authorization policies, like **WHO** wants access to **WHAT** from **WHERE**, **WHEN**, and **WHY**.

# Attribute Based Access Control (ABAC)

The diagram given below describes the ABAC principle.



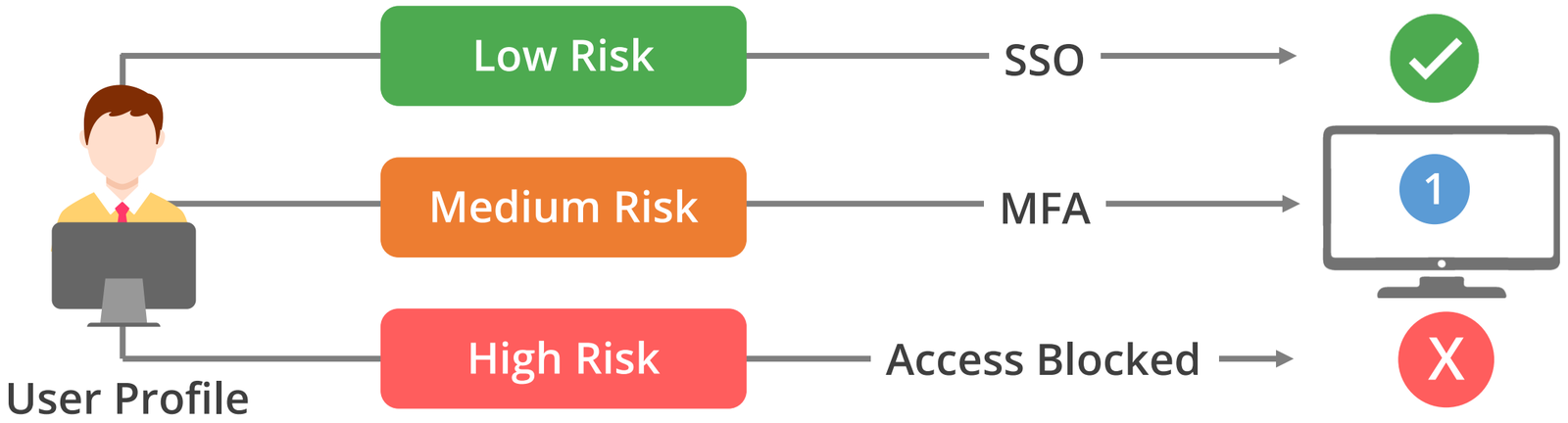
# RBAC vs. ABAC

| | Role-Based Access Control (RBAC) | Attribute-Based Access Control (ABAC) |
|---|---|---|
| **Access** | Access is based on roles | Access is based on attributes |
| **Distributed environment** | • Not well suited<br>• Even more difficult when subject and resource belong to different security domains | • Well suited 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 | Security labels can be treated as attributes |
| **Complexity** | Simpler than ABAC | It 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

Risk-based access control model is a dynamic authentication method that takes into account the security risk value related to each access request as a criterion to determine access decisions.

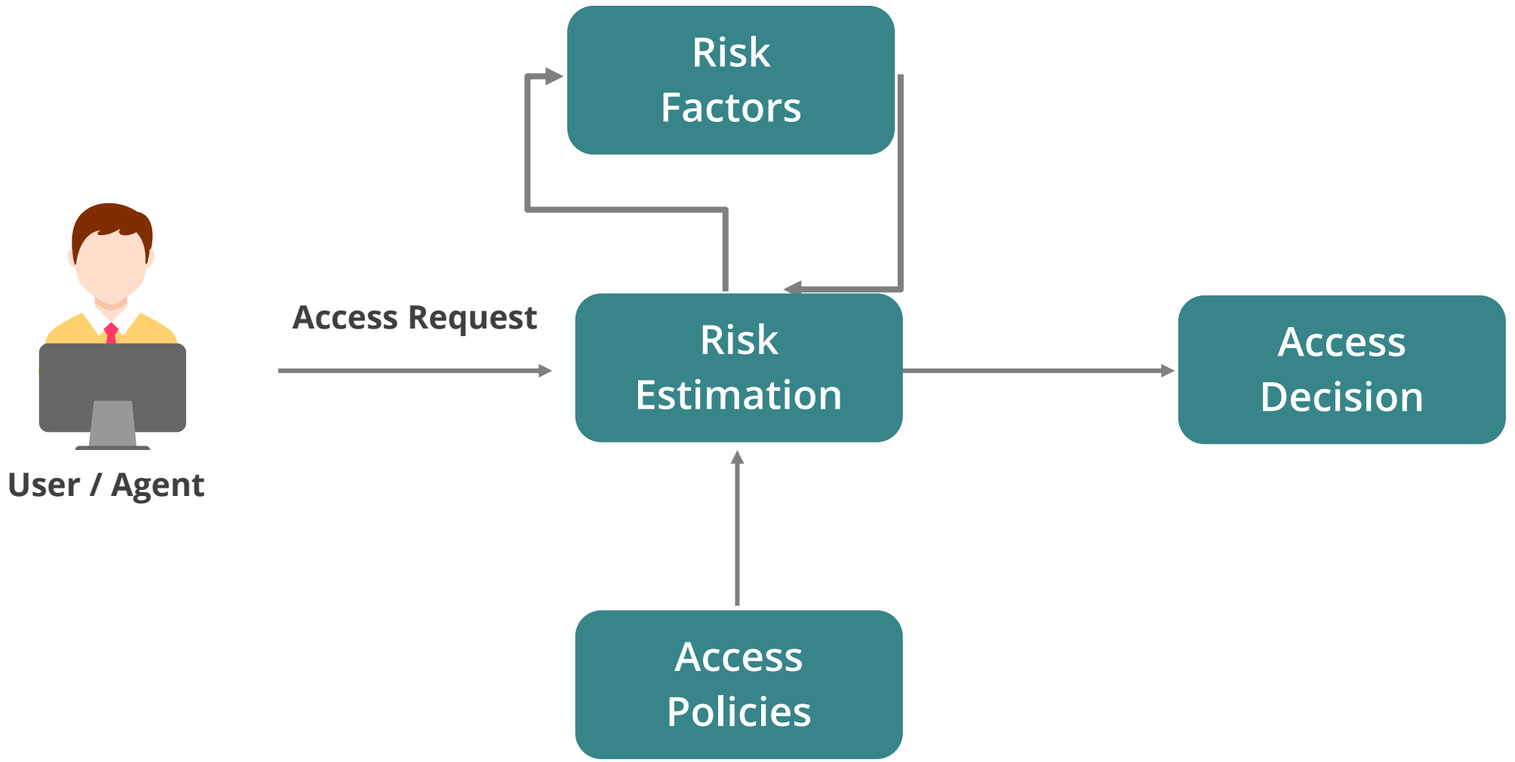
- Users authenticating from known devices, locations, and networks with low risk score could be automatically signed in.
- Suspicious users are required to provide additional credentials using MFA.
- Access request with a high risk score would be denied access.




Information source: https://www.youtube.com/watch?v=elAHAt95QQk

# Risk-Based Access Control

Main elements of a risk-based access control model:



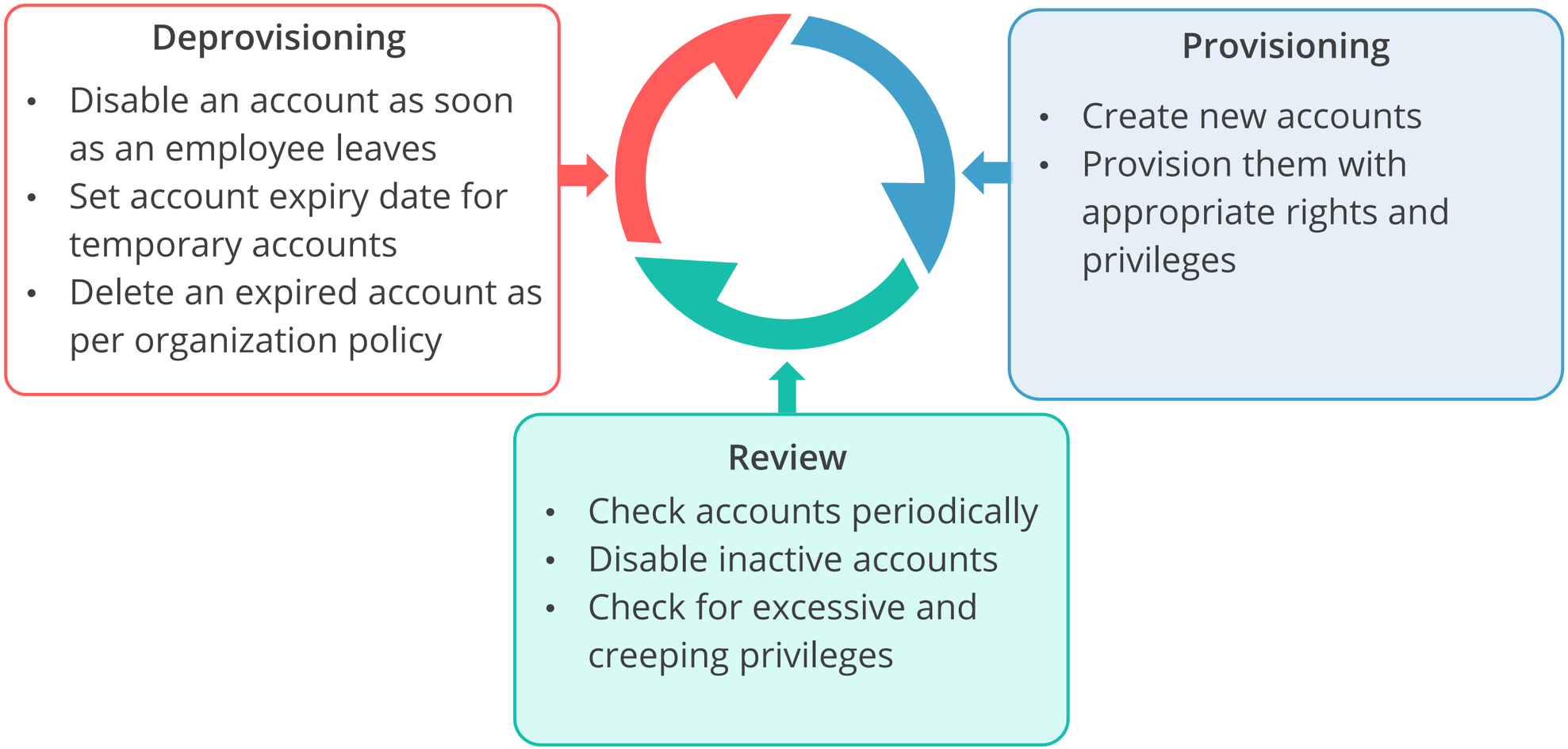
# Manage the Identity and Access Provisioning Lifecycle

# Account Access Review

- User access review is a periodic review of access rights for all organization's employees and vendors. This can help identify excessive or creeping privileges.
- Service accounts are accounts created specifically to be used by services, applications, and virtual machines. The service accounts usually have elevated privileges and access to business-critical applications and data.
- Policies generally dictate when these accounts should be reviewed, deactivated, or deleted.
- Regular review or audit of the service accounts will help identify unusual behaviors that may indicate a breach or misuse.

# Identity and Access Provisioning Lifecycle

The identity and access provisioning lifecycle must be maintained and secured.



# Role Definition

A role is defined as a set of one or more permissions that can be assigned to a user who will inherit these permissions.

A permission is used to grant users the ability to perform an action on a resource.

A user can belong to one or more roles.

Assignment of roles and permissions to a user must follow the principle of least privilege and need to know.

# Privileged Accounts

- A privileged account is defined as an account that has more privileges than normal user accounts.
- Superuser accounts are highly privileged accounts, such as administrator (in Windows environments) or root (in Unix or Linux environments).
- In Unix and Linux systems, the sudo command allows a normal user to temporarily gain root privileges for only a single command use.
- Service accounts are accounts created specifically to be used by services, applications and virtual machines.
- Administrators often assign full administrative privileges to these service accounts without considering the principle of least privilege. If an attacker manages to compromise the application, they can potentially gain full administrative privileges of the service account.

# Privilege Escalation

- Privilege escalation occurs when a malicious user is able to gain higher level of permissions, access, or privileges than they have been assigned.
- Privilege escalation can occur due to administrative oversight, through identity theft or credential compromise, such as keystroke capturing or password cracking.

# Privilege Escalation

## Horizontal privilege escalation

Occurs when an attacker gains rights and privileges of another user with similar privileges. This action is referred to as **account takeover**.

## Vertical privilege escalation

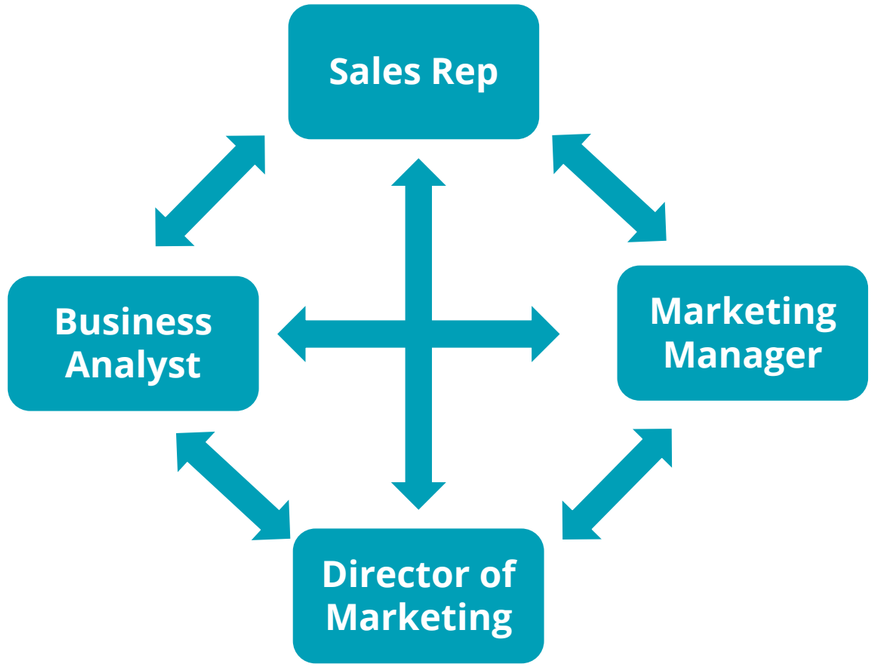
Occurs when an attacker gains access to an account and then tries to elevate the privileges of the account. This is also known as a **privilege elevation attack** and entails moving from a low-level of privileged access, to a higher level of privileged access.

Information source: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

# Privilege Escalation

While each user above has only a standard user account, each also has different spheres of access that encompass different assets and credentials. Some of those credentials may be shared with other/assets, allowing lateral movement and horizontal escalation.
An internal horizontal escalation attack can occur between each of those accounts.
An outside attacker can also achieve horizontal escalation by compromising one of these accounts.

**Horizontal Privilege Escalation Attack**

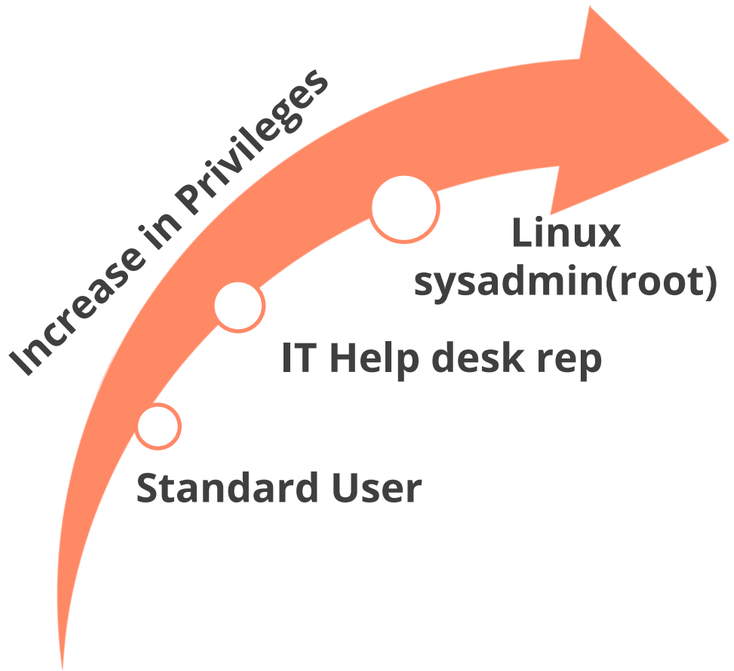



Information source: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

# Privilege Escalation

In this vertical escalation attack, a threat actor moves from standard user access to an IT Help Desk account before gaining Linux sysadmin (root) access. Each subsequent step represents more privileged access and an example of vertical privilege escalation

**Vertical Privilege Escalation Attack**




Information source: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

# Privilege Escalation

Measures to minimize privilege escalation attacks:

Use multi-factor authentication


Minimize the number and scope of the privileged accounts

Follow the principle of least privilege

# Privilege Escalation

Measures to minimize privilege escalation attacks:

Enable continuous monitoring of privileged accounts, and keep detailed log of their activities

Analyze each privileged user or account to identify and address any risks, potential threats, sources, and attacker's intents

Prevent sharing of privileged accounts and credentials

# Implement Authentication Systems

# OpenID Connect

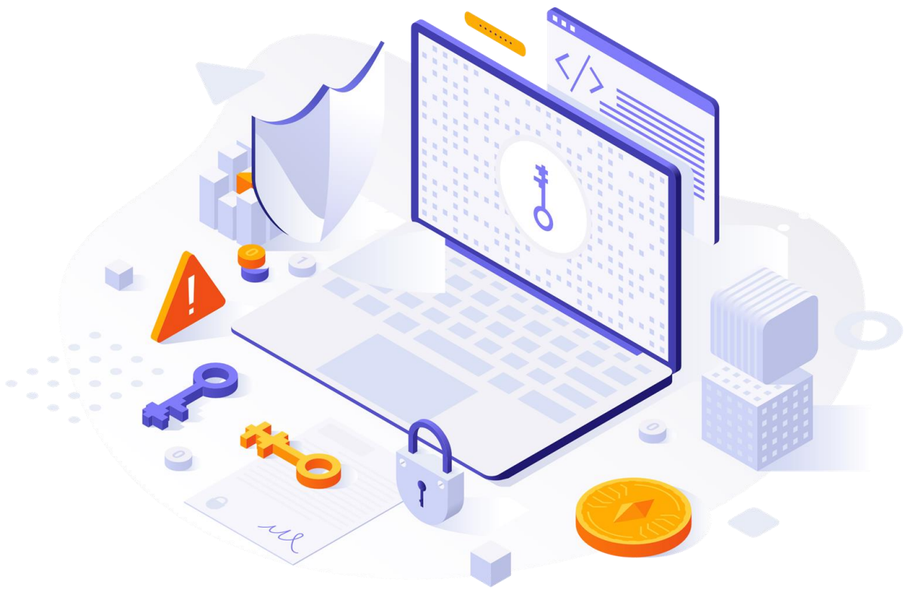
**OpenID**

- It allows you to use an existing account to sign into multiple websites without needing to create new passwords.
- You may choose to associate information with your OpenID that can be shared with the websites you visit, such as a name or an email address. With OpenID, you control how much of that information is shared with the websites you visit.
- With OpenID, your password is only given to your identity provider and that provider then confirms your identity to the websites you visit.
- Other than your provider, no website ever sees your password. So you don't need to worry about an unscrupulous or an insecure website compromising your identity.

# OAuth

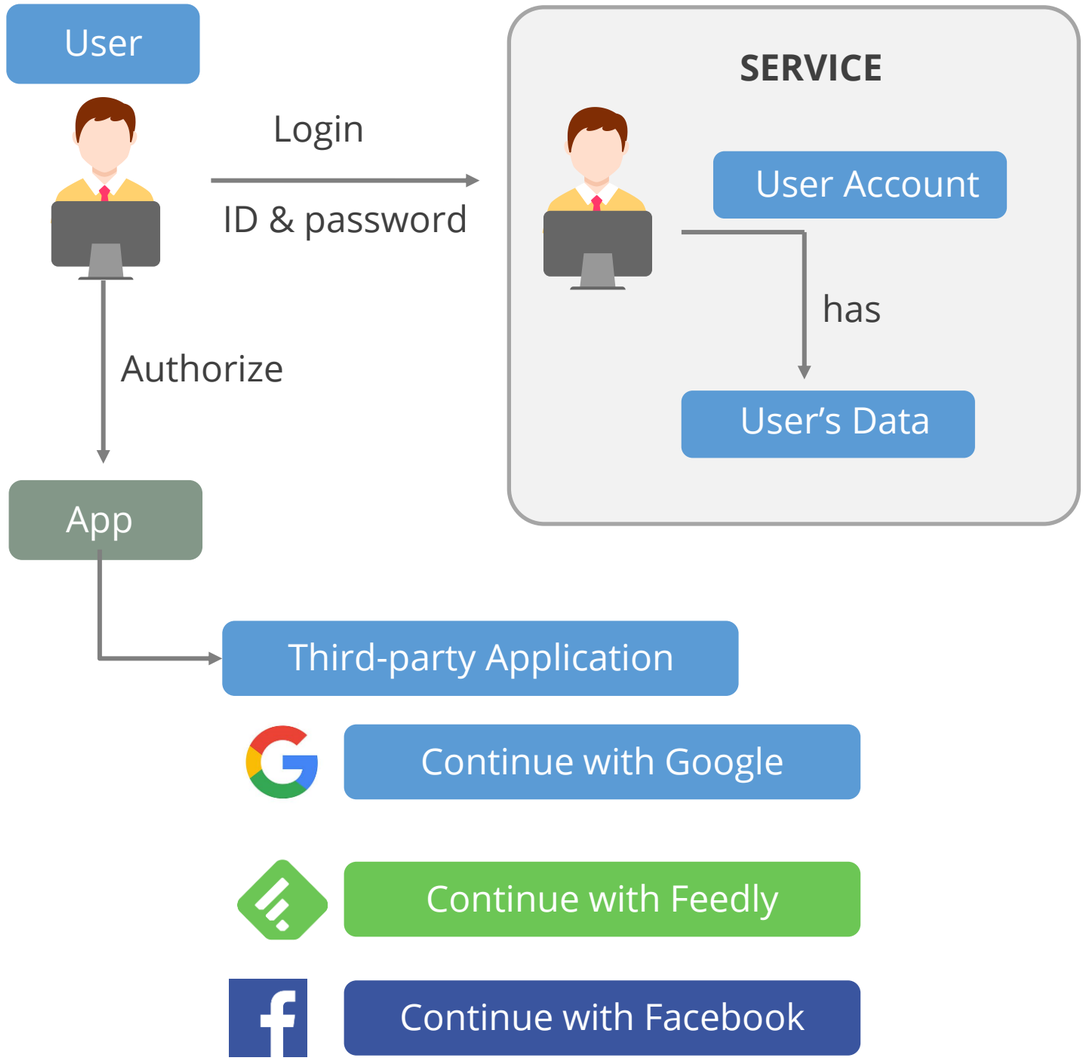
- OAuth is an open-standard authorization protocol or framework that describes how unrelated servers and services can safely allow authenticated access to their assets without actually sharing the initial, related, and single login credentials.

- In the authentication parlance, this is known as a secure, third-party, user-agent, and delegated authorization.



# OAuth: Example

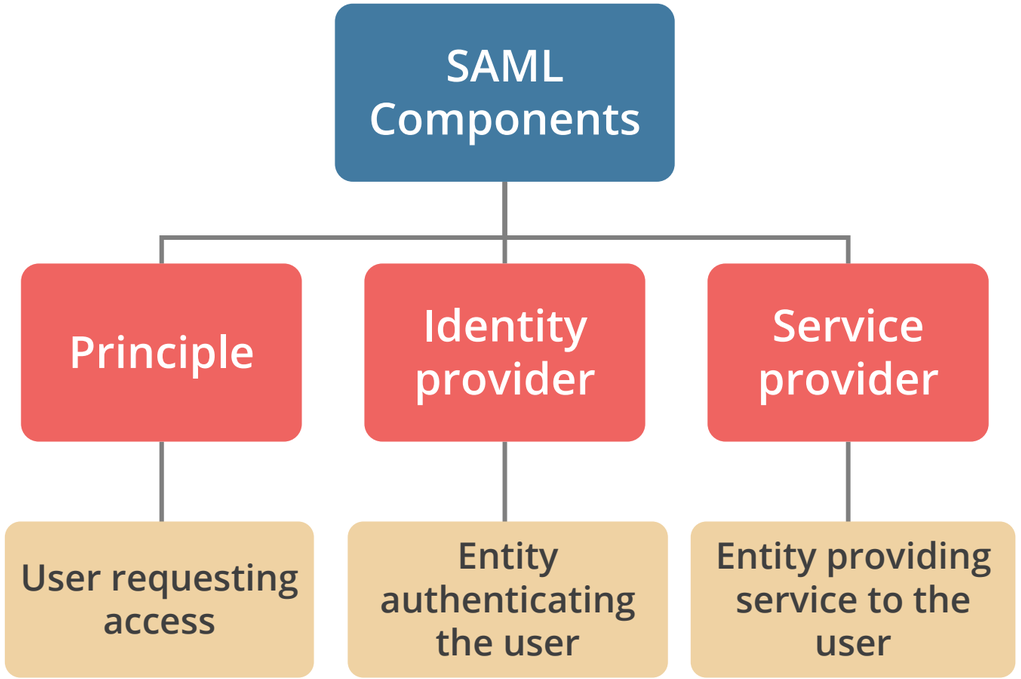
- The simplest example of OAuth is when you login to a website and it offers one or more opportunities to login using another website or service login.
- You then click on the button linked to the other website, the other website authenticates you, and the website you were originally connecting to logs you in itself after using **permission gained** from the second website.



# Security Assertion Markup Language (SAML)

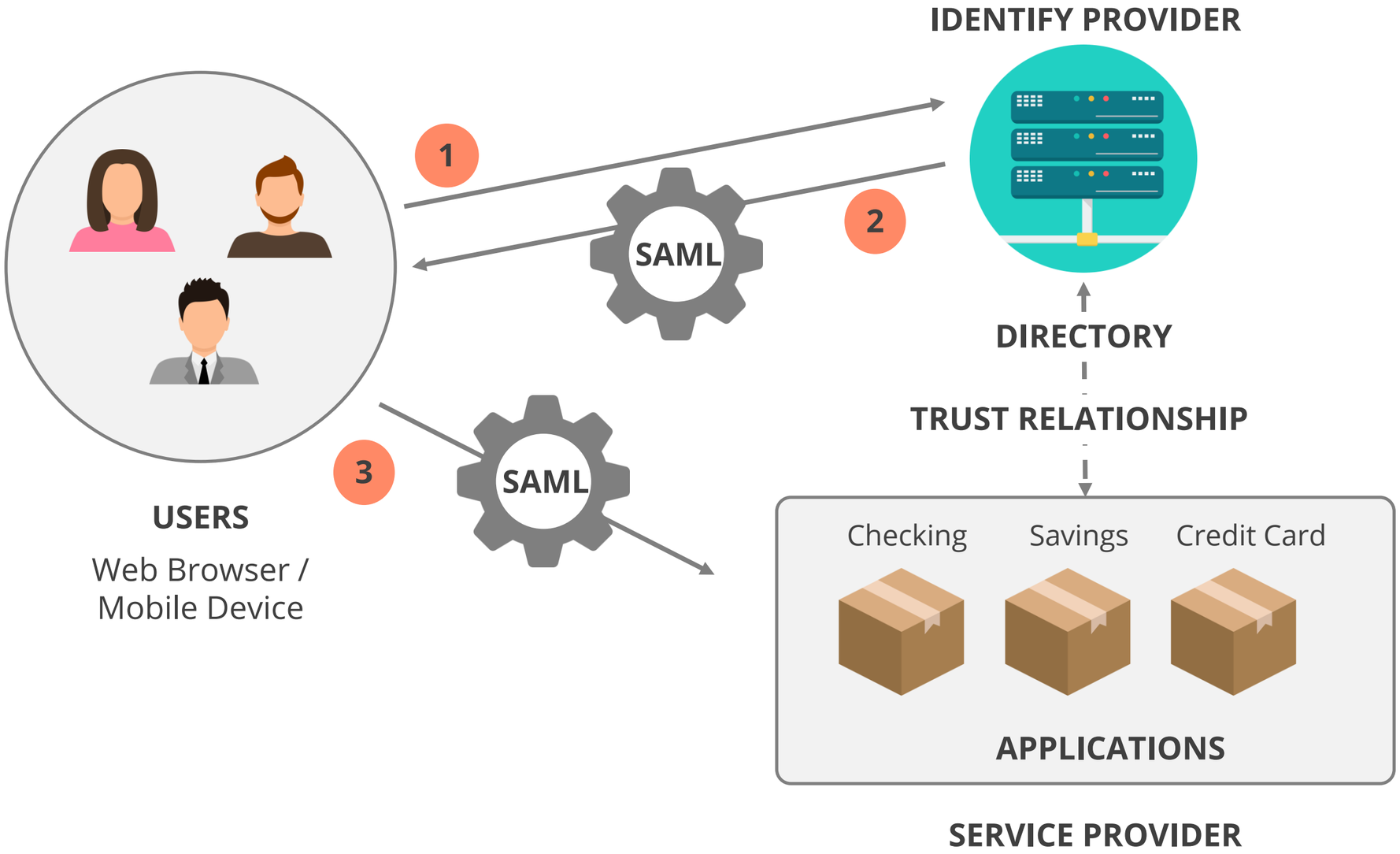
## Security Assertion Markup Language (SAML)

- It is an XML standard that allows the exchange of authentication and authorization data between security domains.
- It provides the authentication pieces to the federated identity management systems.
- Federated identity systems often use SAML and SPML for access needs.
- It is used to provide SSO capabilities to access different browsers.
- SAML does not have a security mode, and it relies on TLS for message confidentiality and digital signature for message integrity.



# Security Assertion Markup Language (SAML)

The diagram given below will help to understand SAML.



# Difference between SAML, OAuth and OpenID

| | SAML 2.0 | OAuth2 | 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 |

# Kerberos

Kerberos is an authentication protocol used for network-wide authentication. Kerberos:

- Is based on symmetric key cryptography
- Provides end-to-end security
- Has the following roles

# Kerberos

**Key Distribution Center (KDC)**

KDC stores secret keys of all services and users. It consists of authentication server (AS) and ticket granting server (TGS).

**Authentication Server (AS)**

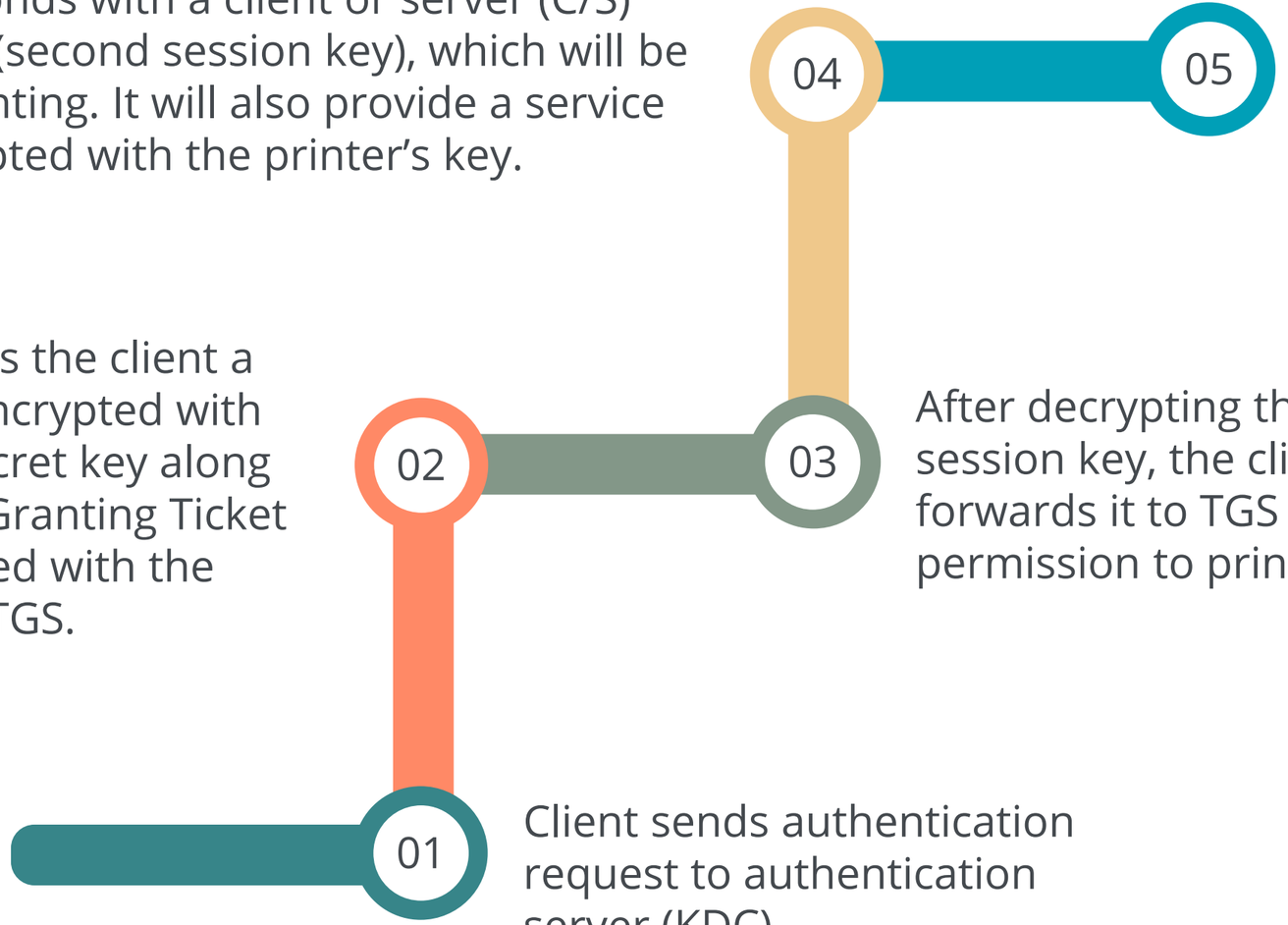
AS authenticates identities of subjects on the network.

**Ticket Granting Server (TGS)**

TGS generates unique session keys between two entities. The session keys are then used by the entities for message encryption.

# Kerberos Steps

When a user wishes to log on to the network and access a print server, the following steps are performed:




Client sends authentication request to authentication server (KDC).

The KDC sends the client a session key encrypted with the client's secret key along with a Ticket Granting Ticket (TGT) encrypted with the secret key of TGS.

After decrypting the session key, the client forwards it to TGS to get permission to print.

With a valid session key with the client, the TGS server responds with a client or server (C/S) session key (second session key), which will be used for printing. It will also provide a service ticket encrypted with the printer's key.

The client sends the tokens to the printer with a valid C/S session key. This proves its authenticity and the server permits the client to print.

# Problems with Kerberos

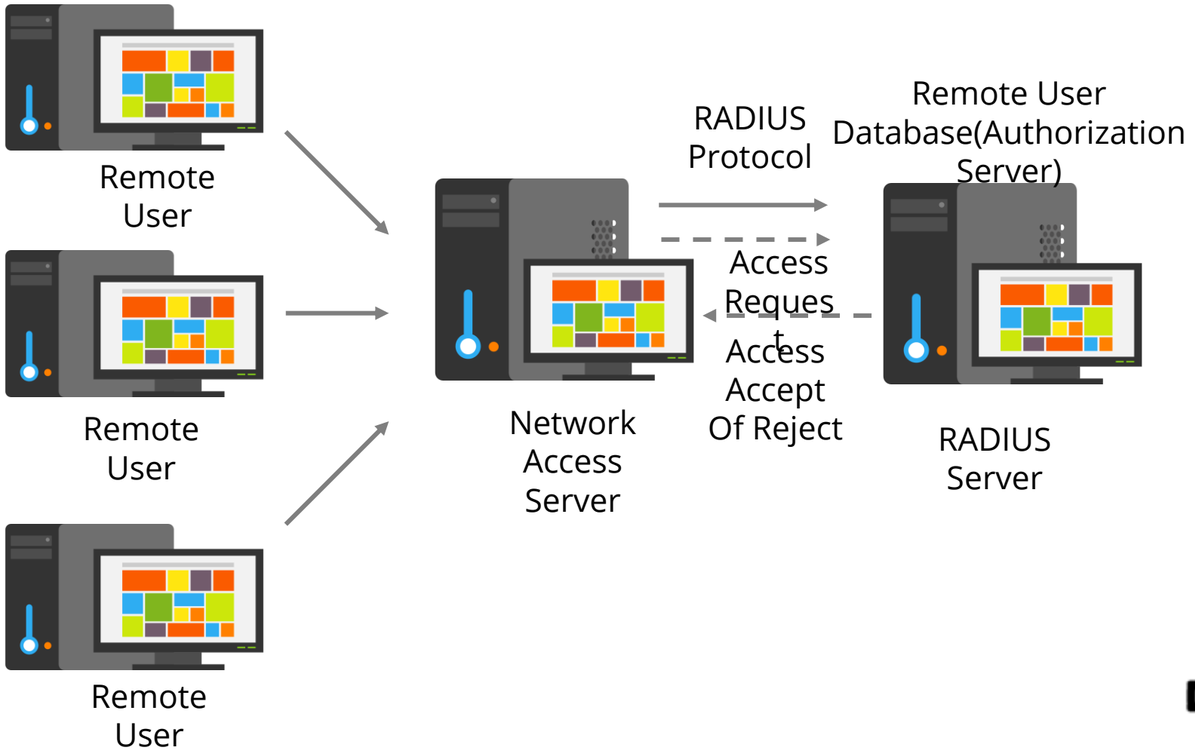
## Drawbacks of Kerberos

- A single KDC is a sole point of failure and performance bottleneck.
- Computers must have clocks synchronized within 5 minutes of each other.
- Secret keys are temporarily stored in the workstation. If compromised, the identity can be forged.
- If KDC is hacked, security is lost.
- It is vulnerable to password guessing attacks.

# Remote Authentication Dial-In User Service (RADIUS)

Remote Authentication Dial-In User Service

- Third-party authentication system
- Client or server authentication protocol used for authenticating and authorizing remote users
- Encrypts only passwords
- Runs in the application layer and uses UDP as transport
- The attribute-value pair (AVP) field uses 8 bits
- Serves three functions: authentication, authorization, and accounting



# TACACS and TACACS+

## Terminal Access Controller Access Control System (TACACS):

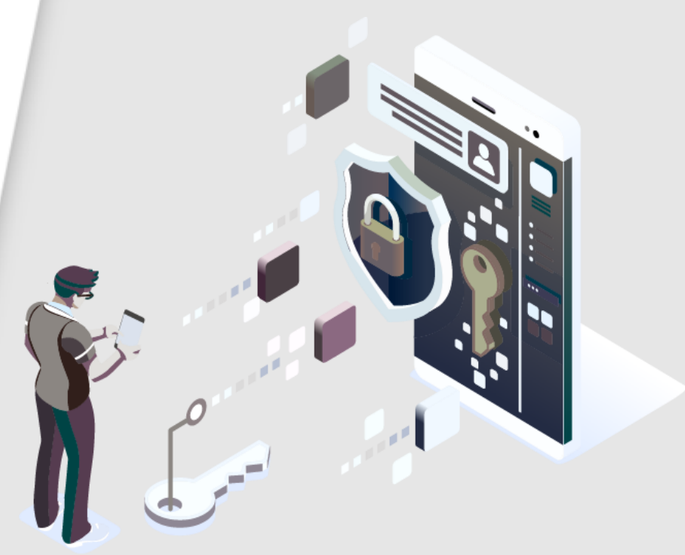
- Is an example of centralized access control system
- For authentication, a user is required to send the user ID along with a password
- UDP port 49 is used

## TACACS+:

- Allows two-factor strong authentication, which gives better password protection
- No backward compatibility with TACACS
- TCP port 49 is used
- For added protection, it can use dynamic (one-time) passwords
- More secure than RADIUS and encrypts all data

# Key Takeaways

- Access controls protect systems and resources from unauthorized access.
- Identity management is the use of different products to identify, authenticate, and authorize the users through automated means.
- Memory cards and smart cards are widely used in identity verification.
- Controls are implemented to mitigate risk and reduce the potential for loss.
- The two types of access control administrations are centralized and decentralized.



This concludes **Identity and Access Management (IAM).**

The next domain is **Security Assessment and Testing.**