Microsoft

SC-900

Learning path 1:

Describe the concepts of security, compliance, and identity

Learning path agenda

- Describe security and compliance concepts.
- Describe identity concepts.

Module 1: Describe security and compliance concepts

Module 1 introduction

After completing this module, you'll be able to:

1 Describe the shared responsibility and the defense in depth security models.

2 Describe the Zero Trust model.

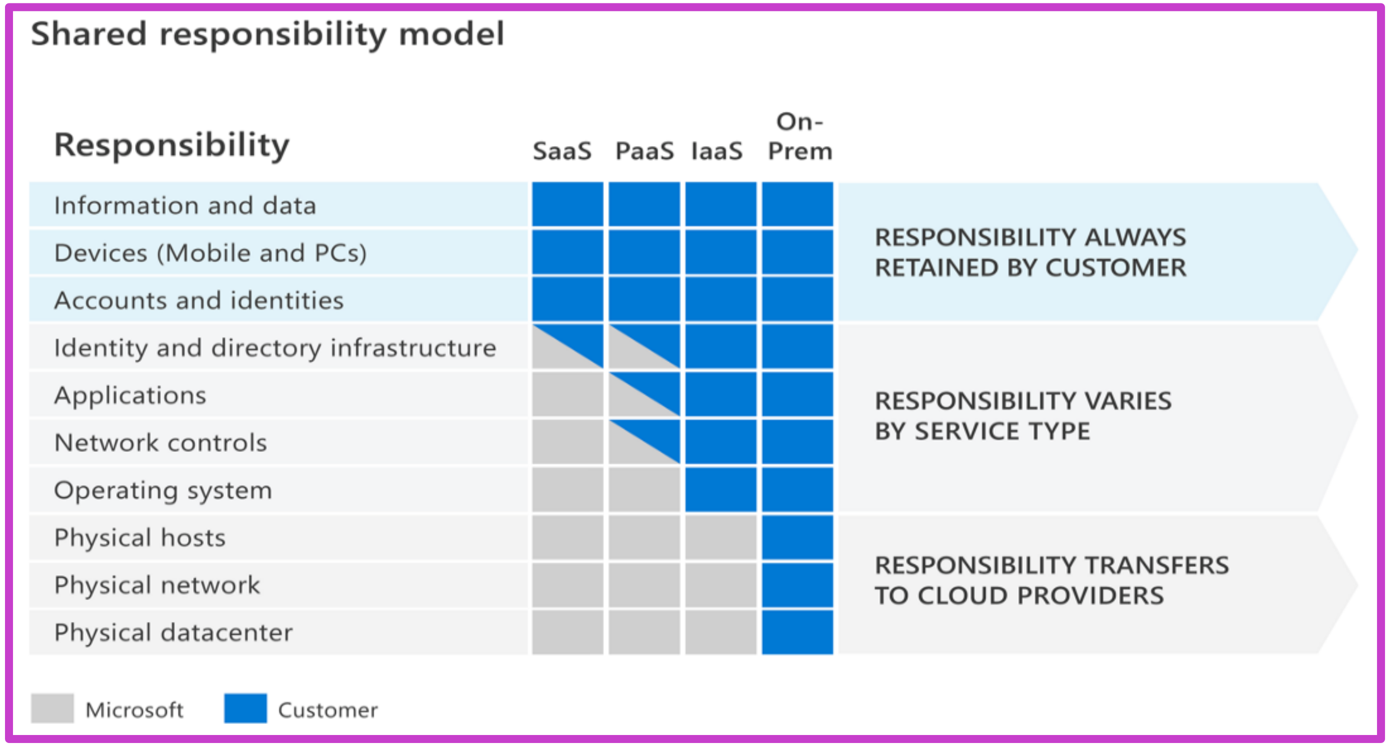
3 Describe the concepts of encryption and hashing.

4 Describe some basic compliance concepts.

The shared responsibility model

The responsibilities vary based on where the workload is hosted:

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)
- On-premises datacenter (On-prem)



Shared responsibility model

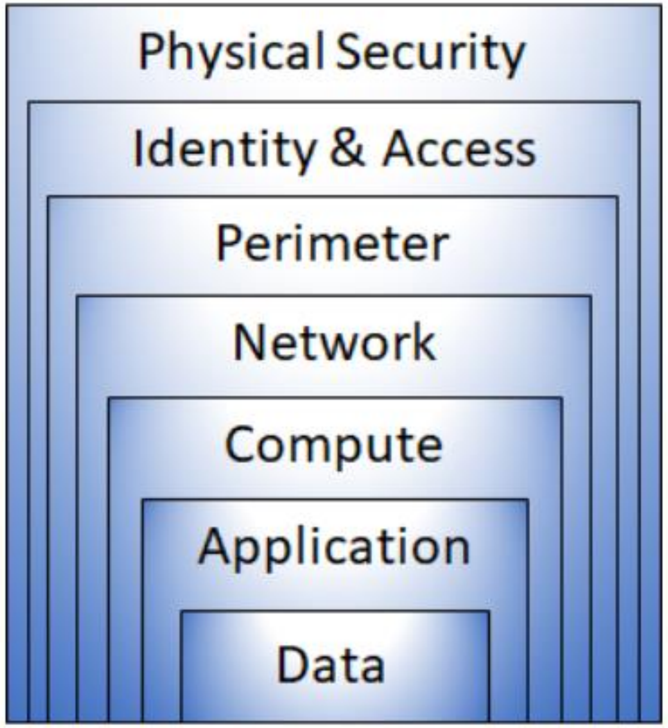
Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	🟦	🟦	🟦	🟦	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦	
Accounts and identities	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	⬜🟦	⬜🟦	🟦	🟦	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	⬜	⬜🟦	🟦	🟦	
Network controls	⬜	⬜🟦	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Physical hosts	⬜	⬜	⬜	🟦	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDERS
Physical network	⬜	⬜	⬜	🟦	
Physical datacenter	⬜	⬜	⬜	🟦	

⬜ Microsoft 🟦 Customer

Defense in depth

Defense in depth uses a layered approach to security. Examples include:

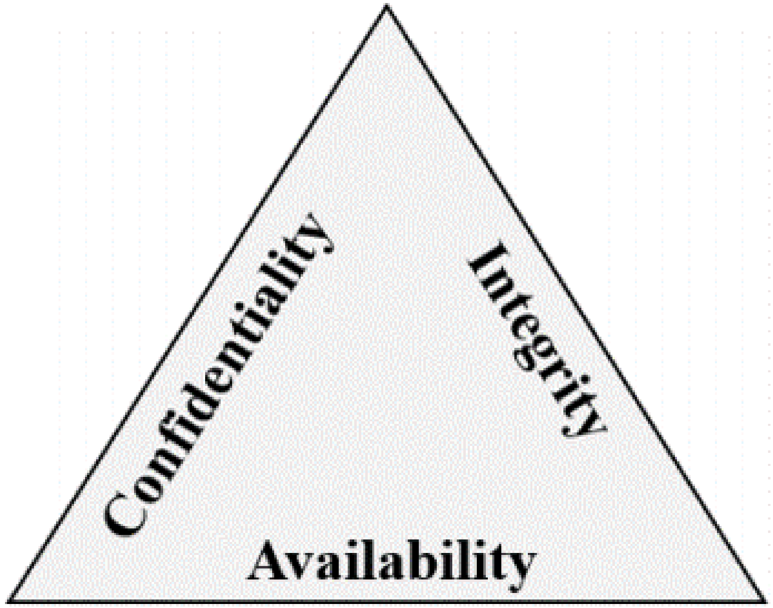
- **Physical security**: Limiting access to a datacenter to only authorized personnel.
- **Identity and access security:** Controlling access to infrastructure and change control.
- **Perimeter security:** Distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a disruption for users.
- **Network security:** Limit communication between resources using segmentation and access controls.
- **Compute layer security:** Securing access to virtual machines by closing certain ports.
- **Application layer security:** Ensure applications are secure and free of security vulnerabilities.
- **Data layer security:** Control access to business and customer data and use encryption to protect data.



Confidentiality, integrity, availability (CIA)

CIA – the goals of a cybersecurity strategy.

- **Confidentiality** ensuring sensitive data, such as customer information remains confidential.
- **Integrity** ensuring data or messages haven’t been tampered with.
- **Availability** refers to making data available to those who need it.



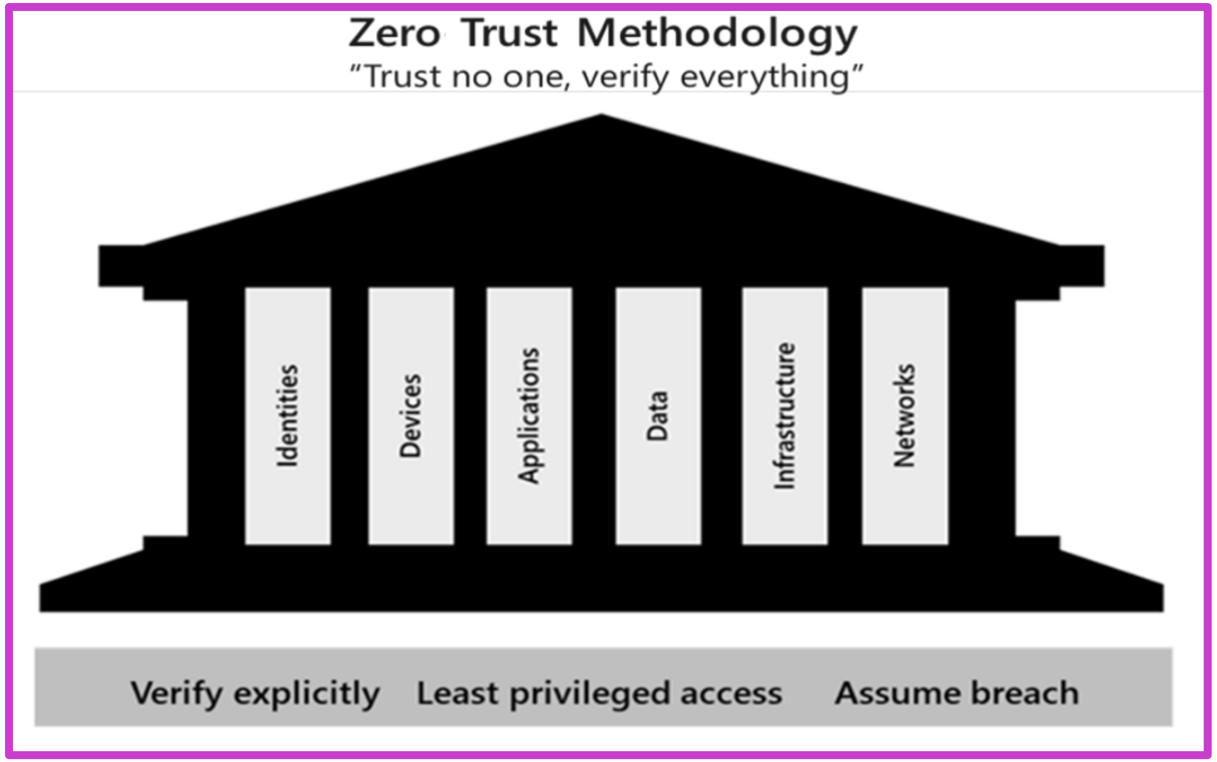
The Zero Trust model

Zero Trust guiding principles

- Verify explicitly
- Least privileged access
- Assume breach

Six foundational pillars

- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Data** should be classified, labeled, and encrypted.
- **Infrastructure**, whether represents a threat vector.
- **Networks** should be segmented.



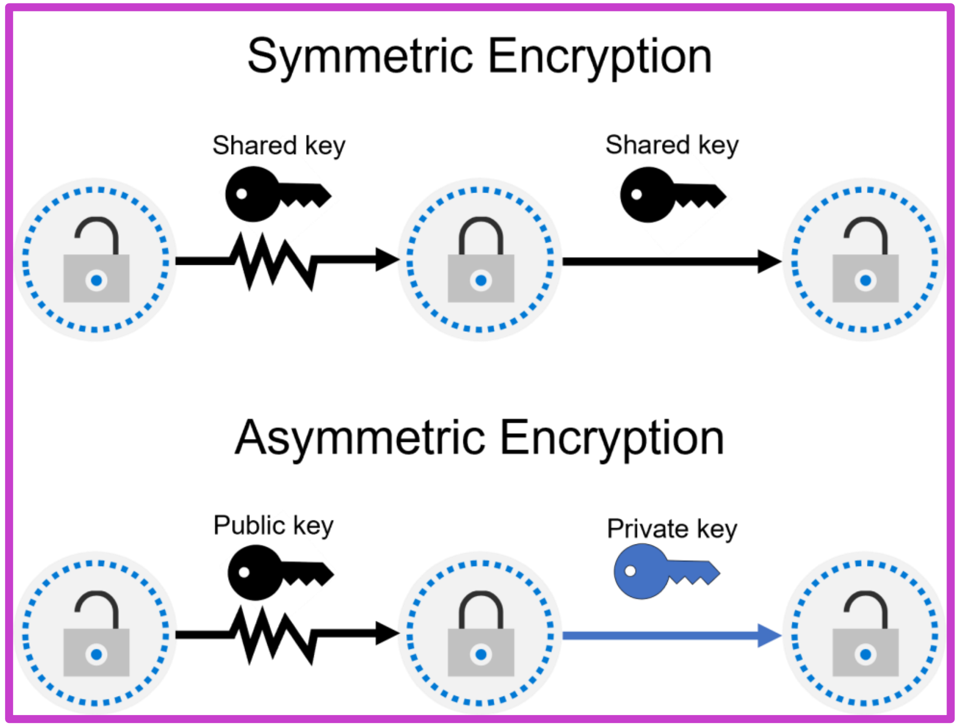
Encryption

Encryption is the process of making data unreadable and unusable to unauthorized viewers.

- Encryption of data at rest.
- Encryption of data in transit.
- Encryption of data in use.

Two top-level types of encryption:

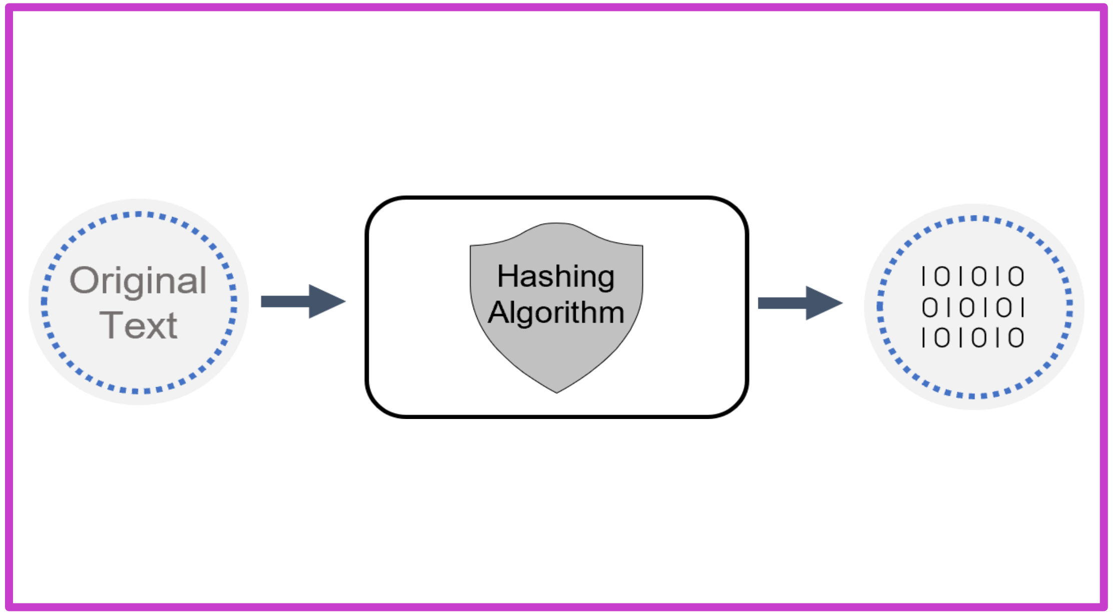
- Symmetric – Uses the same key to encrypt and decrypt data.
- Asymmetric – Uses a public key and private key pair.



Hashing

Hashing uses an algorithm to convert the original text to a *unique* fixed-length hash value. Hash functions are:

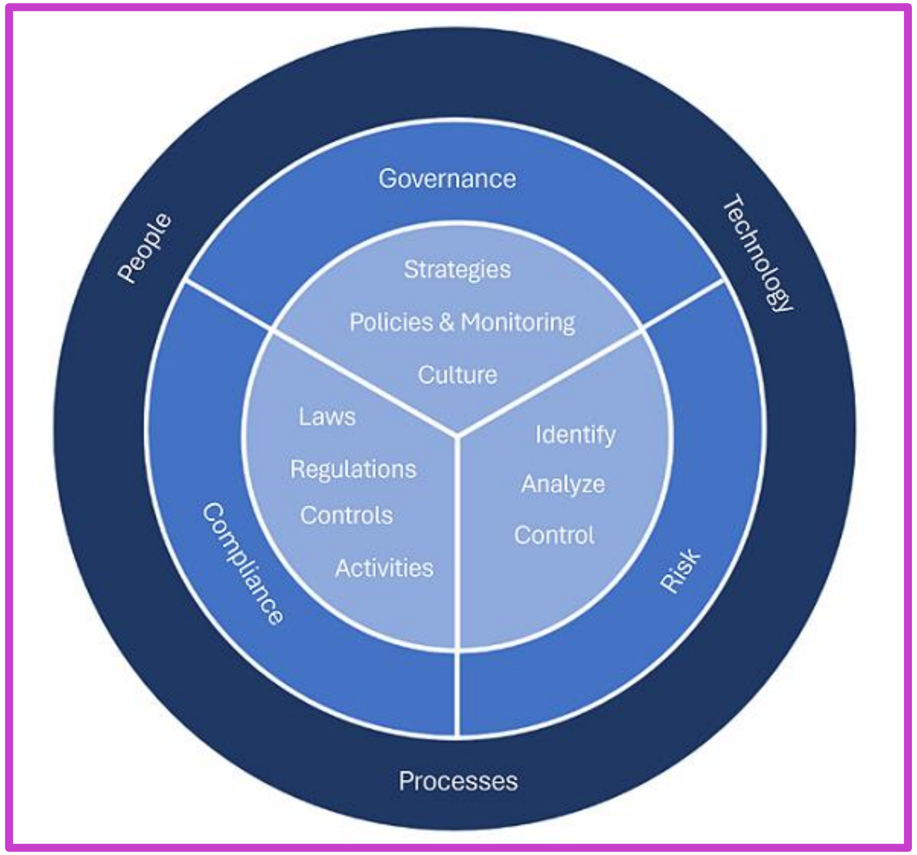
- Deterministic, the same input produces the same output.
- A unique identifier of its associated data.
- Different to encryption in that the hashed value isn't subsequently decrypted back to the original.
- Used to store passwords; the password is "salted" to mitigate risk of brute-force dictionary attack.



Governance, compliance, and risk (GRC) concepts

GRC helps organizations reduce risk and improve compliance effectiveness.

- **Governance** – The rules, practices, and processes an organization uses to direct and control its activities.
- **Risk management** – The process of identifying, assessing, and responding to threats or events that can impact business objectives.
- **Compliance** – The country/region, state or federal laws or even multi-national regulations that an organization must follow.



Module 2: Describe identity concepts

Module 2 introduction

After completing this module, you'll be able to:

1. Understand the difference between authentication and authorization.
2. Describe the concept of identity as a security perimeter.
3. Describe identity-related services

Authentication and authorization

Authentication (AuthN)

Authentication is the process of proving that a person is who they say they are. Authentication ***grants access***.

Authorization (AuthZ)

Authorization determines the ***level of access or the permissions*** an authenticated person has to your data and resources.

Identity as the primary security perimeter

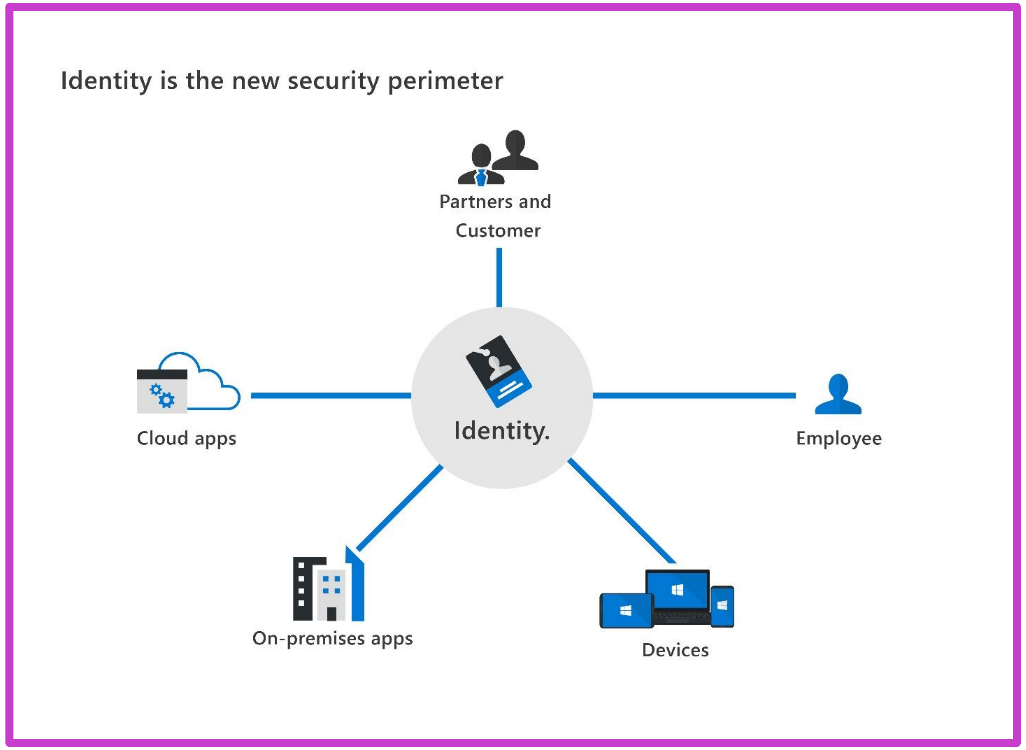
Identity has become the new security perimeter that enables organizations to secure their assets.

An identity, which can be used to authenticate and authorize someone or something, may be associated with:

- User
- Application
- Device
- Other

Four pillars of an identity infrastructure:

- Administration
- Authentication
- Authorization
- Auditing



Modern authentication and the role of the identity provider

Modern authentication **is an umbrella term for authentication and authorization methods between a client and a server.**

1 At the center of modern authentication is the role of the ***identity provider (IdP)***.

2 IdP offers authentication, authorization, and auditing services.

3 IdP enables organizations to establish authentication and authorization policies, monitor user behavior, and more.

4 A fundamental capability of an IdP and "modern authentication" is the support for single sign-on (SSO).

5 Microsoft Azure Active Directory is an example of a cloud-based identity provider.

The concept of directory services

A directory is a hierarchical structure that stores information about objects on the network.

A directory service stores directory data and makes it available to network users, administrators, services, and applications.

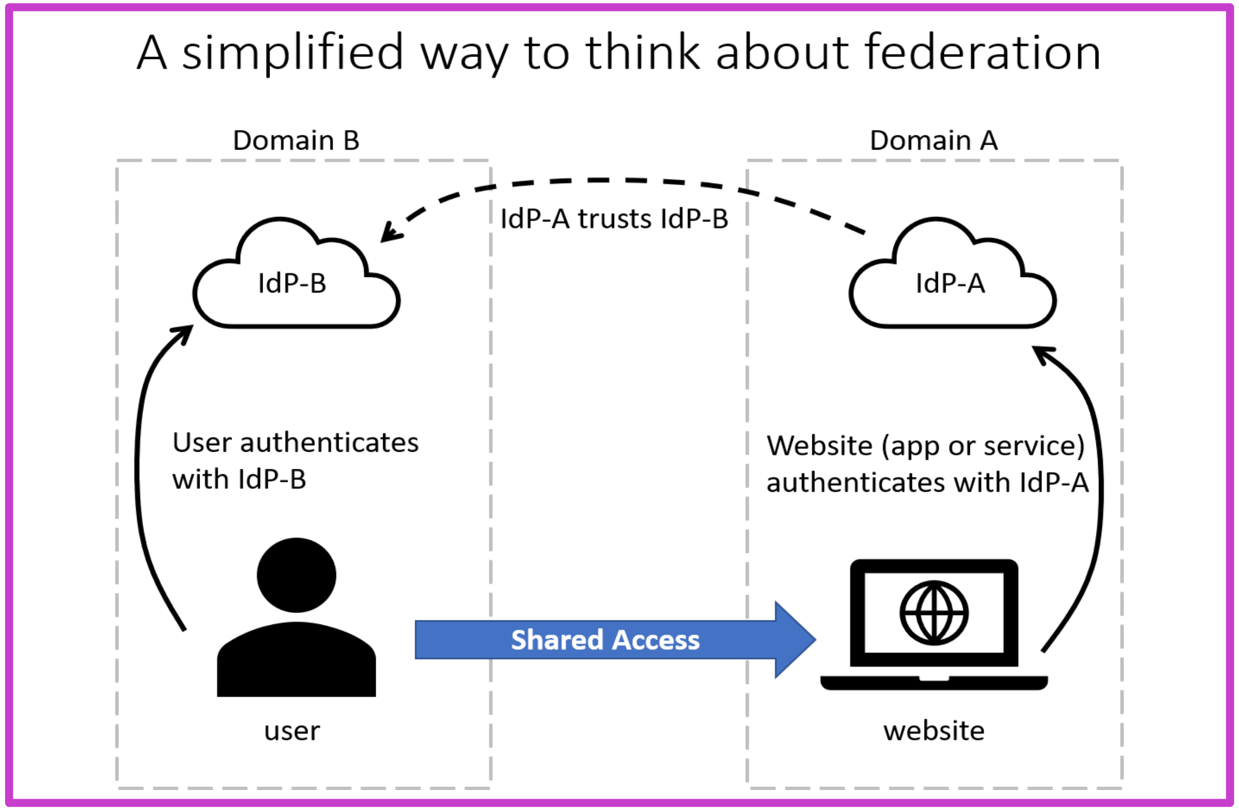
The best-known service of this kind is Active Directory Domain Services (AD DS), a central component in organizations with on-premises IT infrastructure.

Microsoft Entra ID is the evolution of identity and access management solutions, providing organizations with an identity as a service (IDaaS) solution for all their apps across cloud and on-prem.

The concept of federation

A simplified way to think about federation:

- The website uses the authentication services of identity provider A (IdP-A).
- The user authenticates with identity provider B (IdP-B).
- IdP-A has a trust relationship configured with IdP-B.
- When the user signs in to the website, it can trust the user’s credentials and allow access.


A simplified way to think about federation
Domain B
Domain A
IdP-A trusts IdP-B
IdP-B
IdP-A
User authenticates with IdP-B
Website (app or service) authenticates with IdP-A
Shared Access
user
website

Learning path summary

Describe the concepts of security, compliance, and identity.

In this learning path, you have:

- Learned about some important security and compliance concepts including:
  - The shared responsibility model.
  - Defense in depth and how the CIA triad represents the goals of a cybersecurity strategy.
  - The guiding principles and the six foundational elements of the Zero Trust model.
  - The concepts of governance, risk, and compliance (GRC).
- Learned about some important identity concepts, including:
  - Authentication and authorization.
  - Identity as the new security perimeter that enables organizations to secure their assets.
  - The role of an identity provider, directory services, and federation.

Knowledge check

The human resources organization wants to ensure that stored employee data is encrypted. Which security mechanism would they use?

A. Hashing.

B. Encryption in transit.

C. Encryption at rest.

Which of the following best describes the concept of data sovereignty?

A. There are regulations that govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally.

B. Data, particularly personal data, is subject to the laws and regulations of the country/region in which it's physically collected, held, or processed.

C. Trust no one, verify everything.

Knowledge check continued

Which relationship type allows federated services to access resources?

A. Claim relationship.

B. Shared access relationship.

C. Trust relationship.

Authentication is the process of doing what?

A. Verifying that a user or device is who they say they are.

B. The process of tracking user behavior.

C. Enabling federated services.

Microsoft