Microsoft Security

SC-900

Learning Path: Ø1

Describe the Concepts of Security, Compliance, and Identity

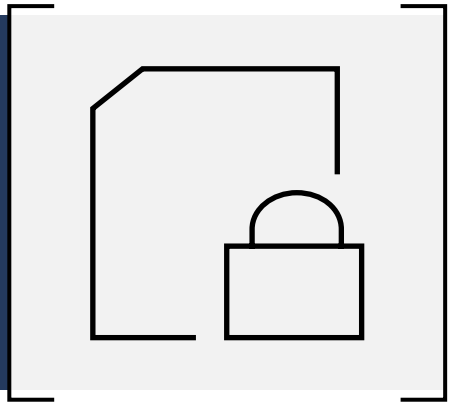
KDC

Learning Path Agenda

Describe security and compliance concepts.

Describe identity concepts.

Module 1: Describe security and compliance concepts



Module 1 Introduction

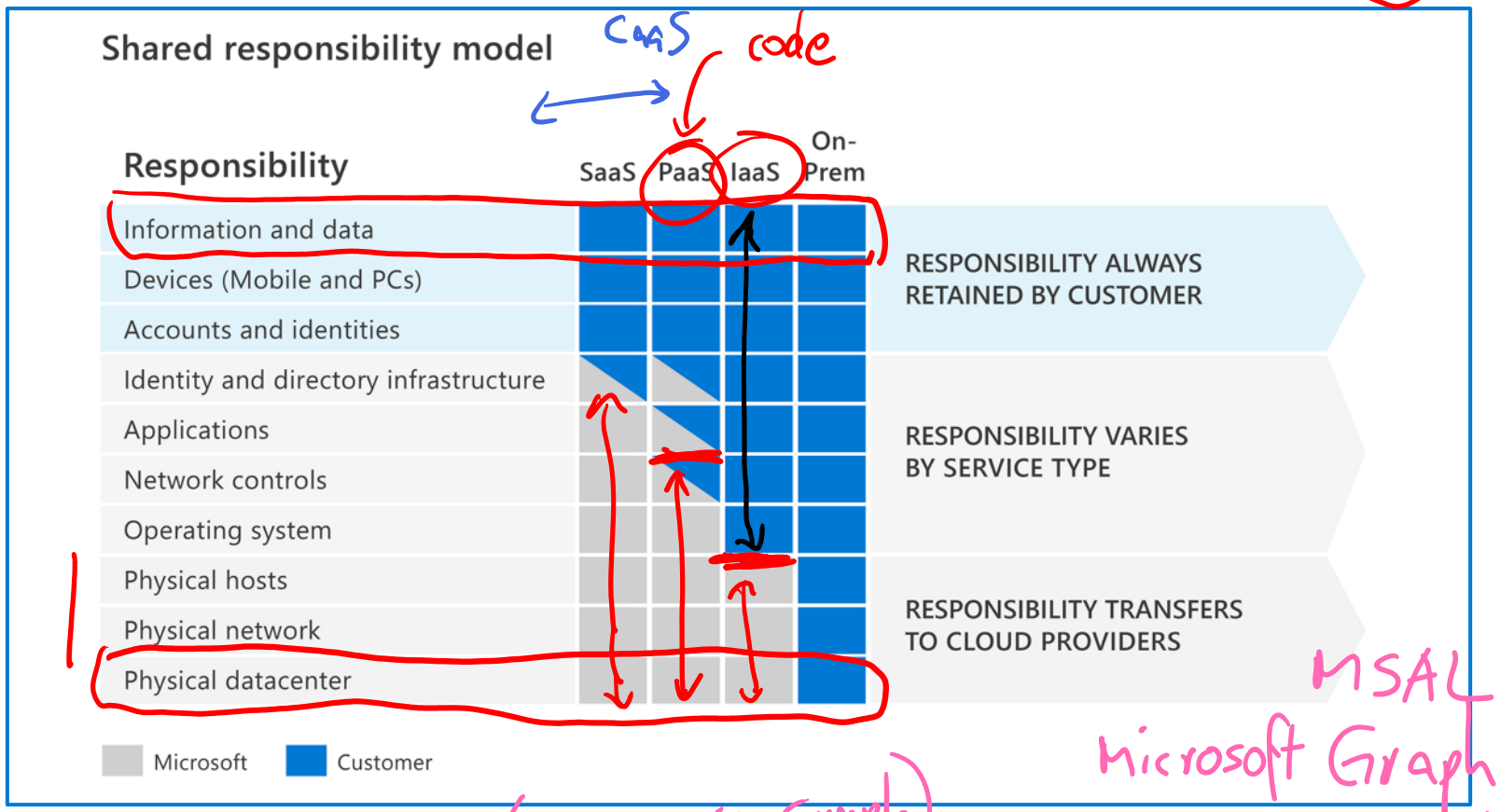
After completing this module, you'll be able to:

- Describe the shared responsibility and the defense in-depth security models.
- Describe the Zero Trust model.
- Describe the concepts of encryption and hashing.
- Describe some basic compliance concepts.

The shared responsibility model

The responsibilities vary based on where the workload is hosted:

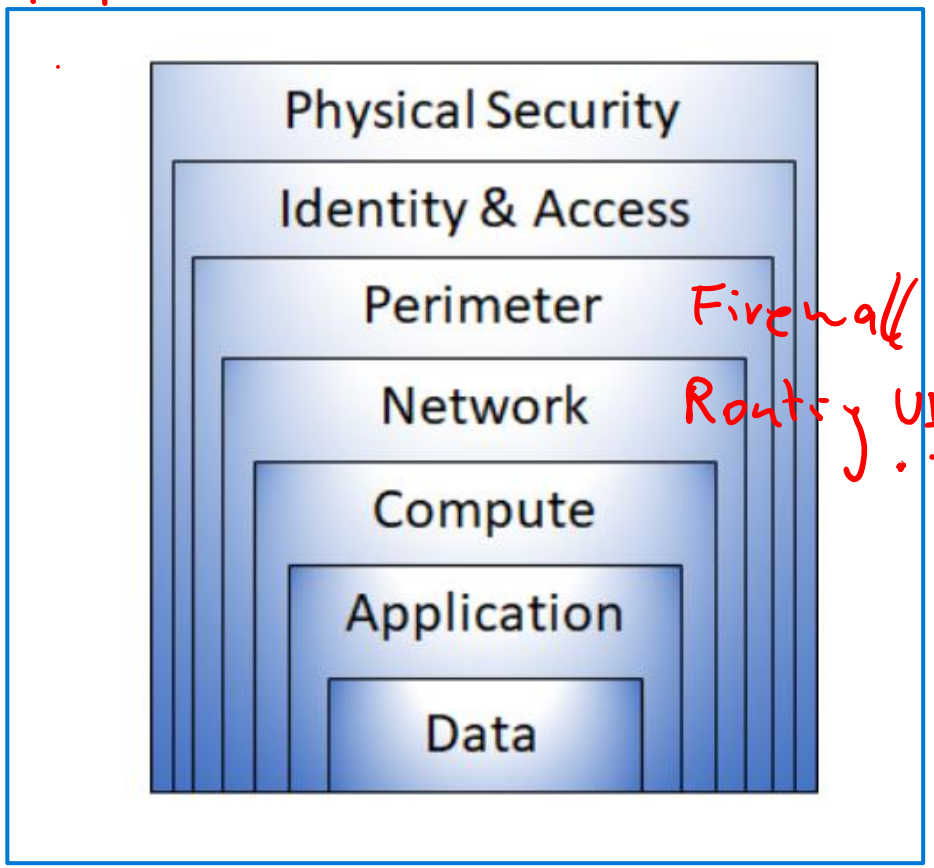
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-Prem)



Defense in depth

Defense in depth uses a layered approach to security:

- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controlling access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security can limit communication between resources using segmentation and access controls.
- **Compute** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security ensures that applications are secure and free of security vulnerabilities.
- **Data** layer security controls access to business and customer data, and encryption to protect data.

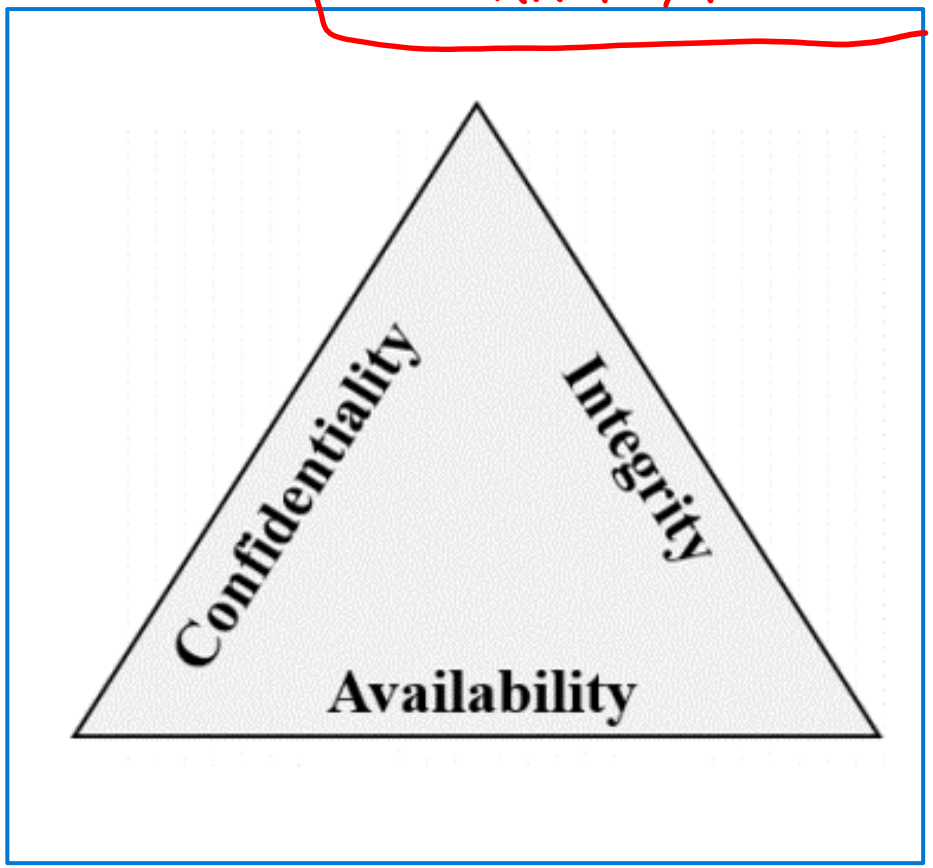


Confidentiality, Integrity, Availability (CIA)

Bicep Lang
↳ ARM Template json
↓
ARM API

CIA – The goals of a cybersecurity strategy.

- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.



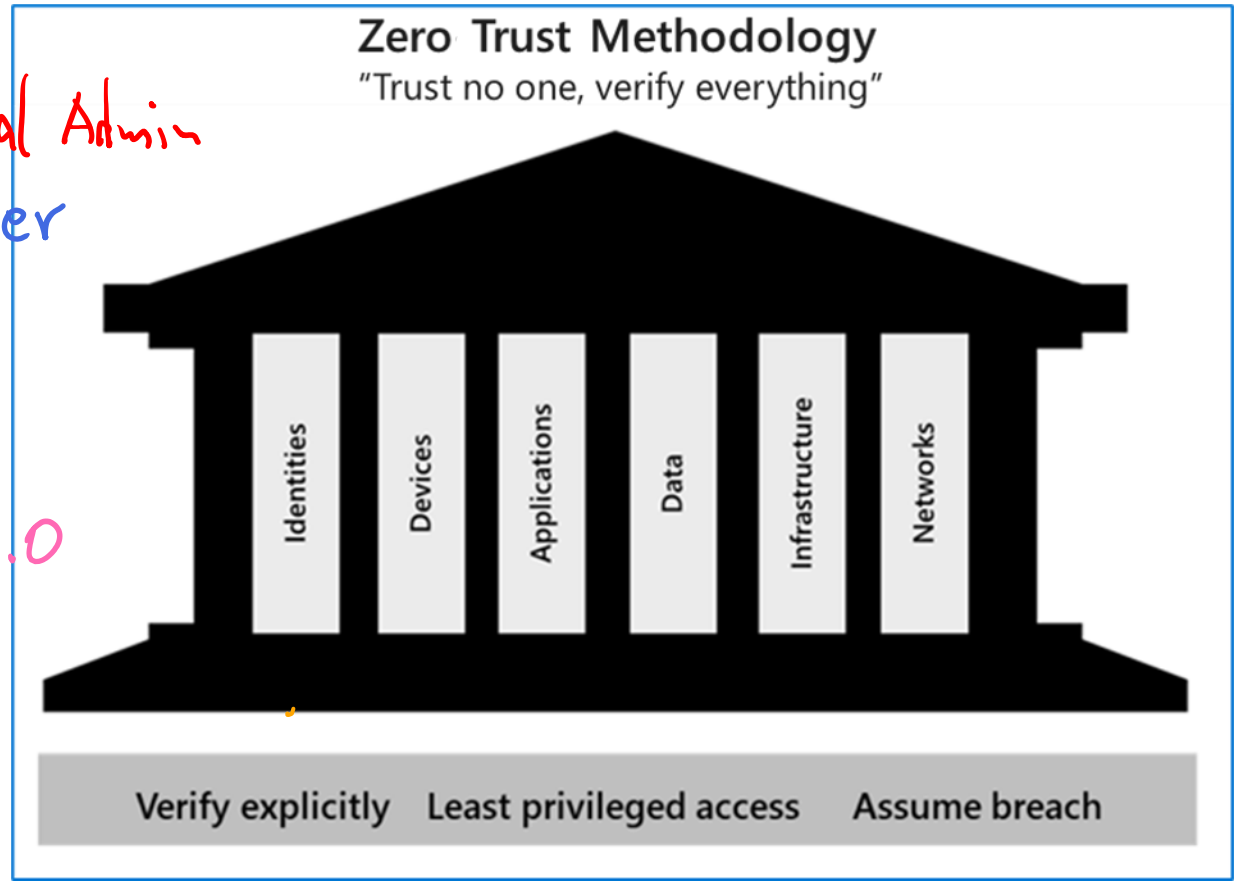
The Zero Trust model

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 based on its attributes.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Networks** should be segmented.



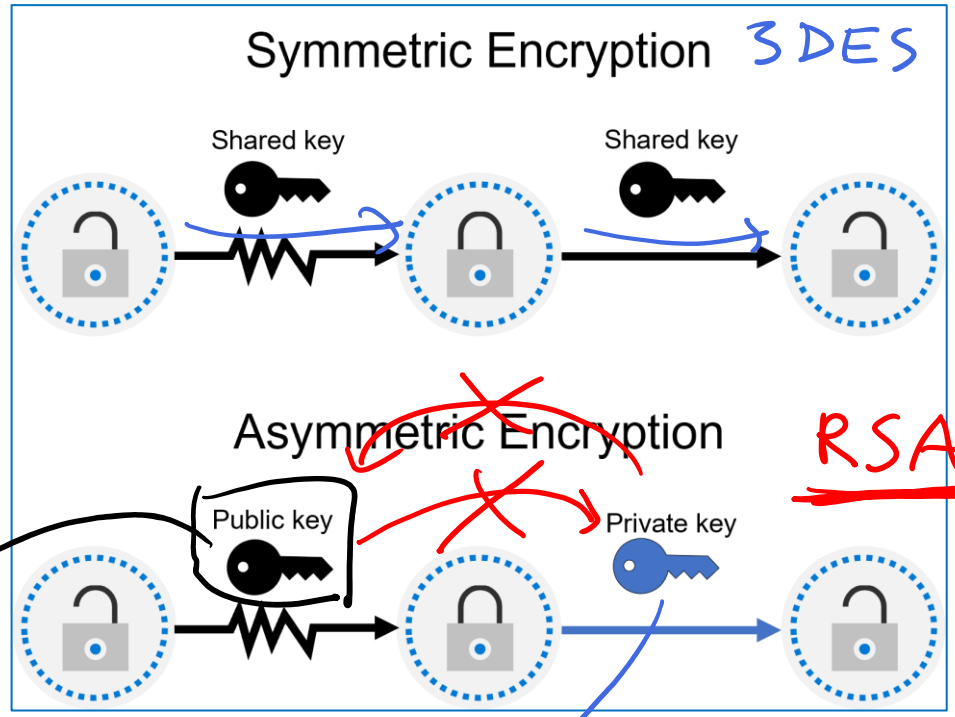
Encryption

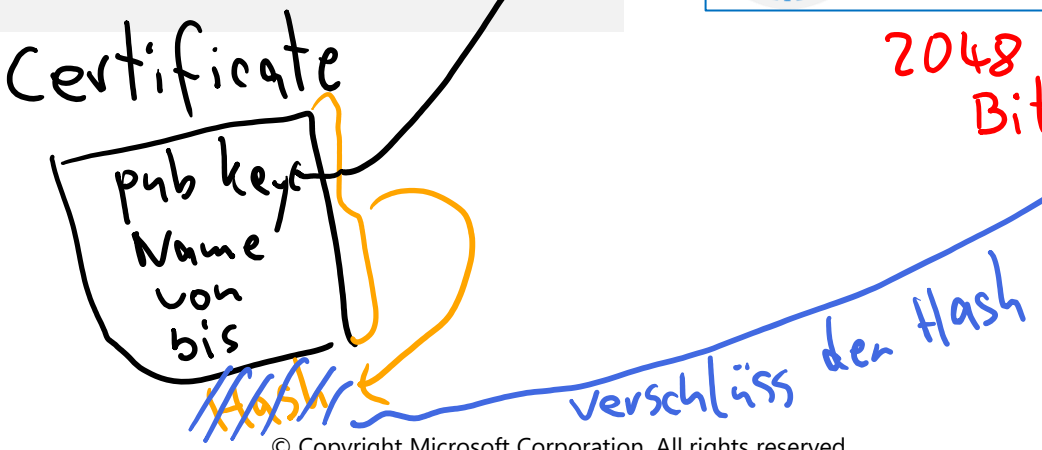
Encryption is the process of making data unreadable and unusable to unauthorized viewers.

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

Two top-level types of encryption:

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



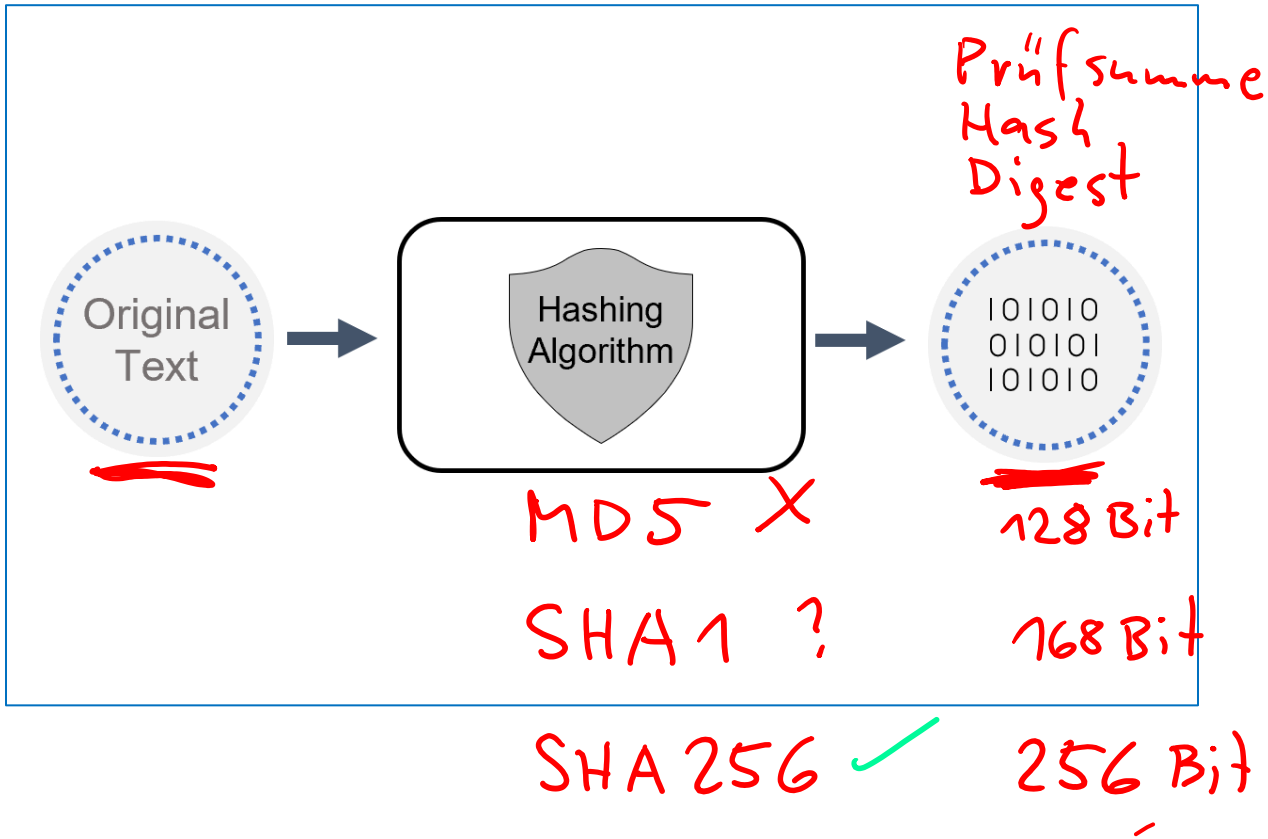


X.509

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.



Compliance concepts

Data residency - Regulations govern the physical locations where data can be stored and how and when it can be transferred, processed, or accessed internationally.

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

Data privacy - Providing notice and being transparent about the collection, processing, use, and sharing of personal data are fundamental principles of privacy laws and regulations.

Module 2: Describe identity concepts

Module 2 Introduction

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

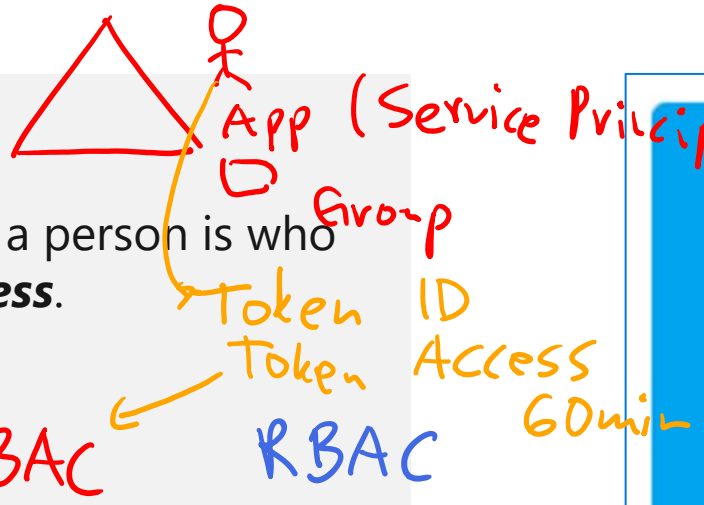
- Understand the difference between authentication and authorization.
- Describe the concept of identity as a security perimeter.
- Describe identity-related services.

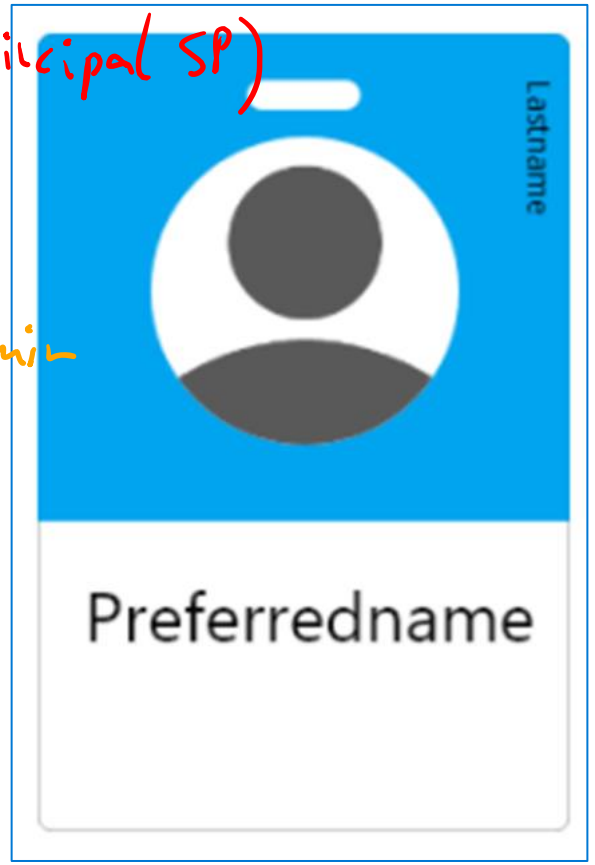
Authentication and authorization

AAA

1. Authentication (AuthN)

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





2. Authorization (AuthZ)

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

3. Accounting | Auditing

Identity as the primary security perimeter

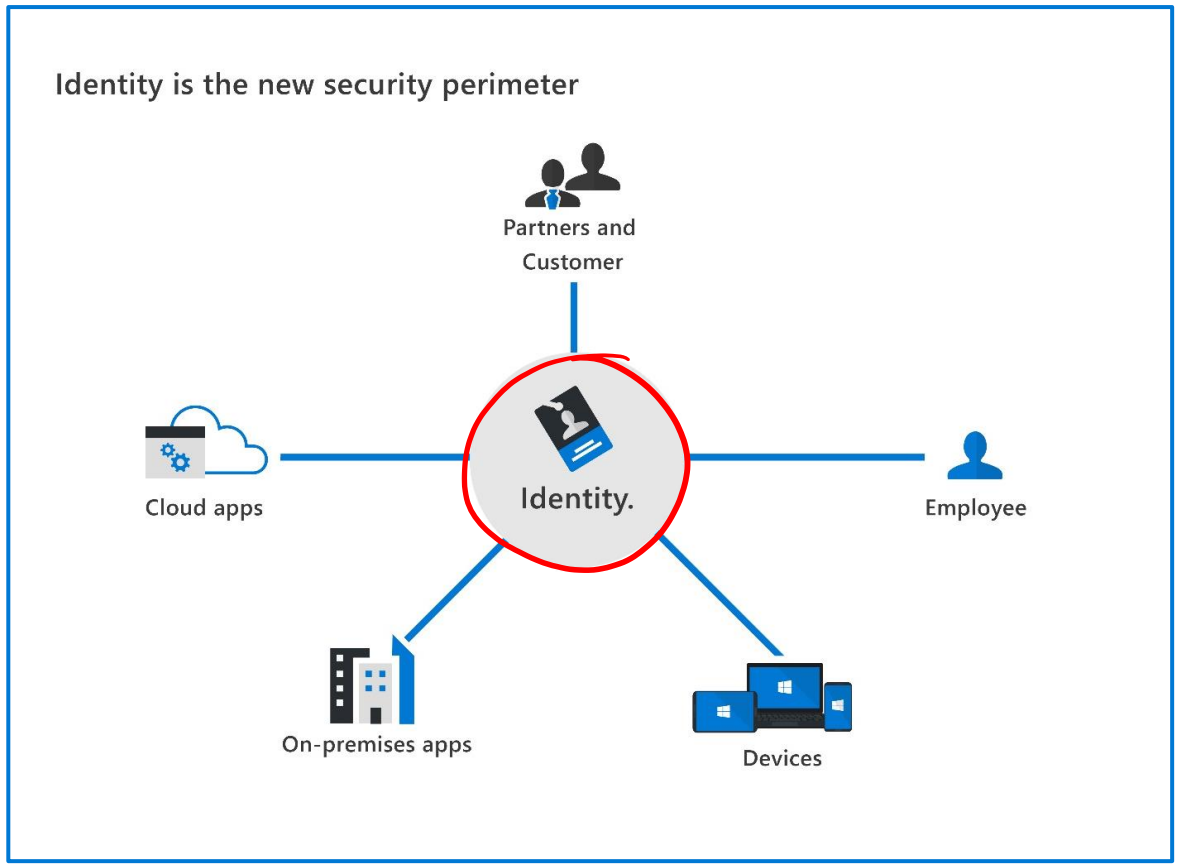
Identity has become the new security perimeter that enables organizations to secure their assets.

An identity is how someone or something can be verified and authenticated and 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.

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

IdP offers authentication, authorization, and auditing services.

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

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

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

The concept of directory services and Active Directory

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.

Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.

The concept of Federation

SAML Token

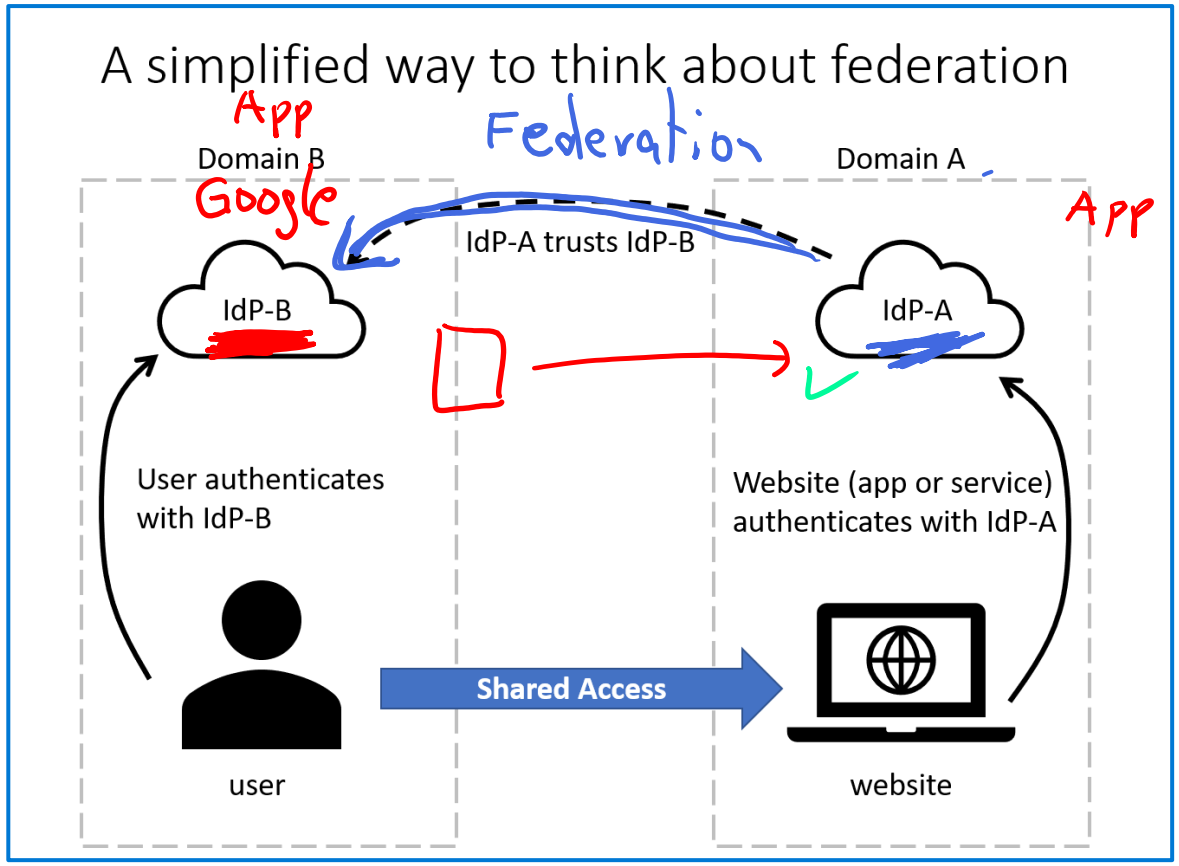
A simplified way to think about federation:

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, the website can trust the user's credentials and allow access.



Learning Path Summary

In this learning path, you have:

- Learned about some important security and compliance concepts.
  - Looked at the shared responsibility model.
  - Learned about defense in depth and how the CIA triad represents the goals of a cybersecurity strategy.
  - Learned about the guiding principles and the six foundational elements that make up the Zero Trust model.
  - Learned about the data compliance concepts of data residency, data sovereignty, and data privacy.
- Learned about some important identity concepts.
  - Learned about authentication and authorization.
  - Learned about the concept of identity as a security perimeter & the four pillars of an identity infrastructure.
  - Learned about identity-related services, including the role of an identity provider, directory services, and federation.

Microsoft Security