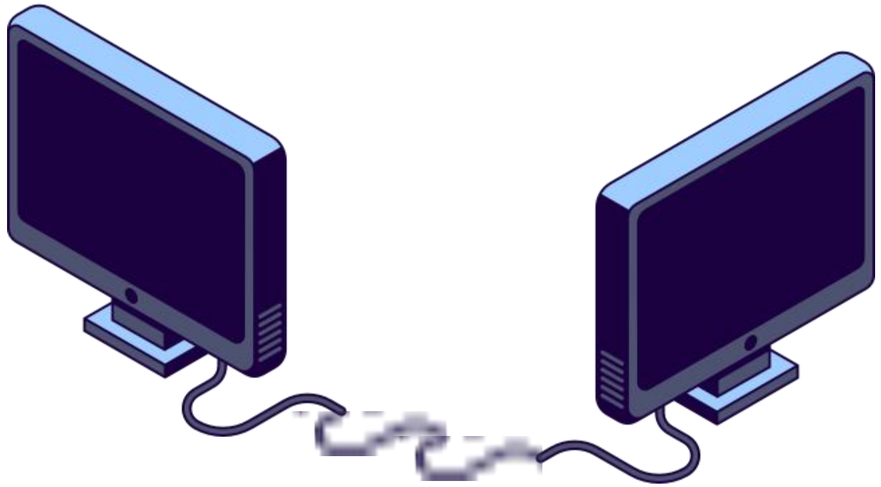
# INTRODUCTION TO NETWORK SECURITY

# WHAT IS NETWORK SECURITY ?

# NETWORKS

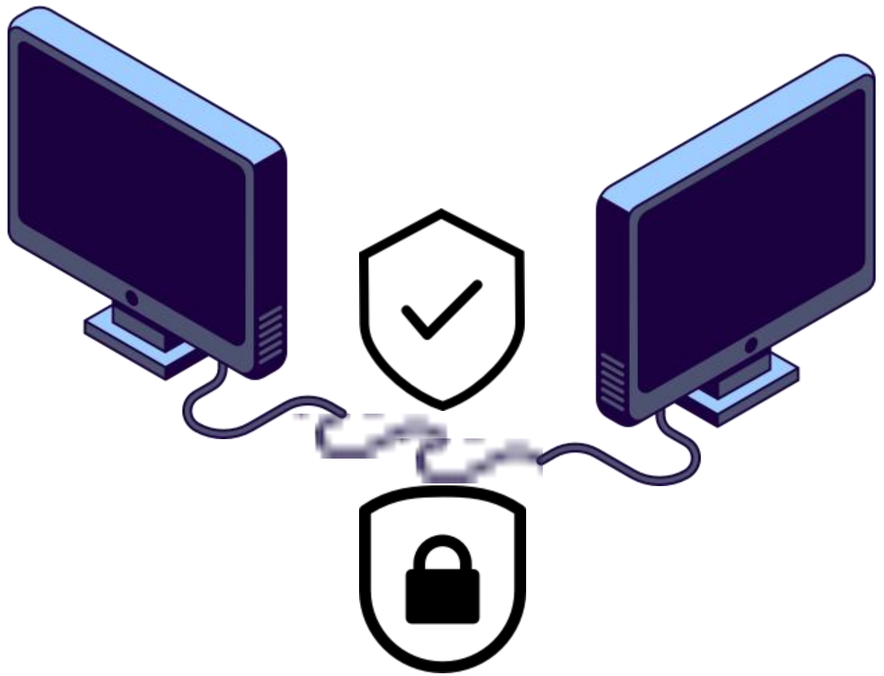
A computer network is two or more computers connected together, allowing them to communicate and share information with each other.



The term ‘computer’ can mean a range of different devices, including laptops, tablets and smartphones.

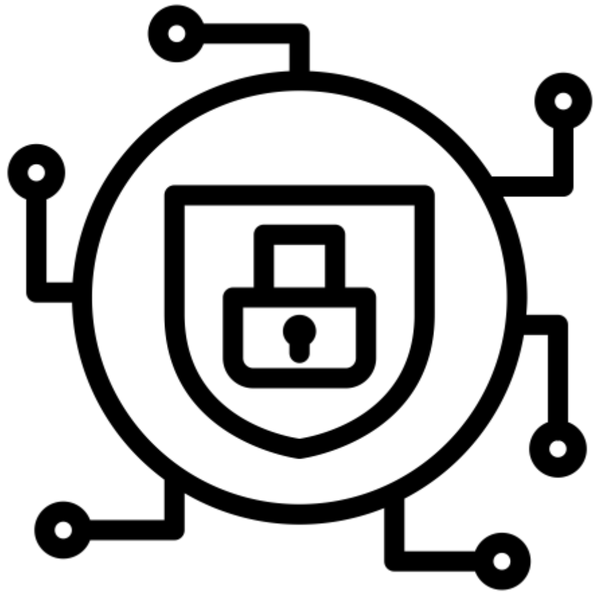
# SECURITY

The protection of a network's infrastructure, data, and assets from unauthorized access, cyberattacks, and data loss.



# WHY NETWORK SECURITY IS IMPORTANT?

- Protects data
- **Prevents cyberattacks**
- **Ensures compliance**
- **Protects reputation**
- **Prevents financial loss**



# COMMON NETWORK SECURITY THREATS

- Malware
- Phishing
- **DoS Attack.**
- **DDoS Attack**
- Man-in-the-Middle Attack
- SQL Injection
- Insider Threat

Question: What does the "A" in CIA Triad stand for?

a) Access
b) Authorization
c) Availability
d) Authentication

# WHAT IS CIA TRIAD ?

## Confidentiality

Protecting data from unauthorized access.

## Integrity

Ensuring data accuracy and reliability

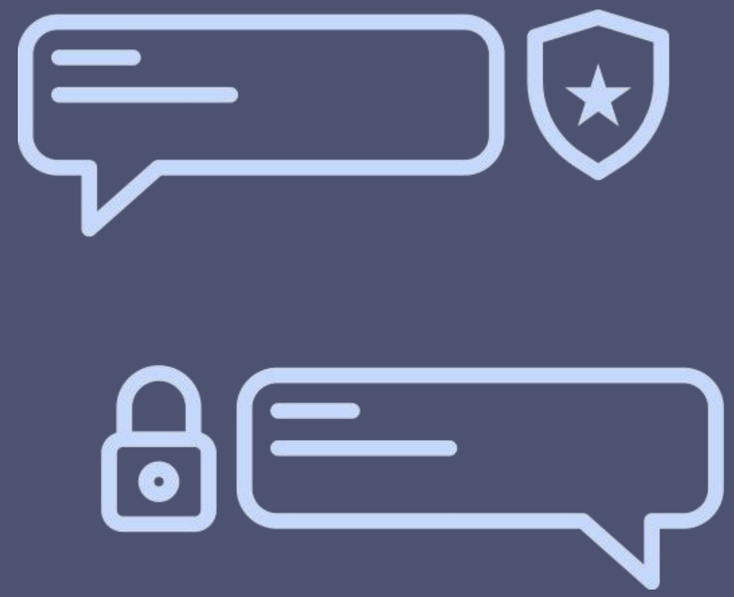
## Availability

Ensuring systems are up and running when needed

# CONFIDENTIALITY IN ACTION

Techniques:

Encryption



# ENSURING INTEGRITY

Techniques:

- Hashing (e.g., SHA-256)
- Digital signatures

# MAINTAINING AVAILABILITY

Techniques:

- Load balancing
- DDoS protection

# Network Protocols for Authentication

- **RADIUS (Remote Authentication Dial-In User Service):**

•Centralized authentication and authorization for network access, commonly used in ISP environments and enterprise Wi-Fi networks.

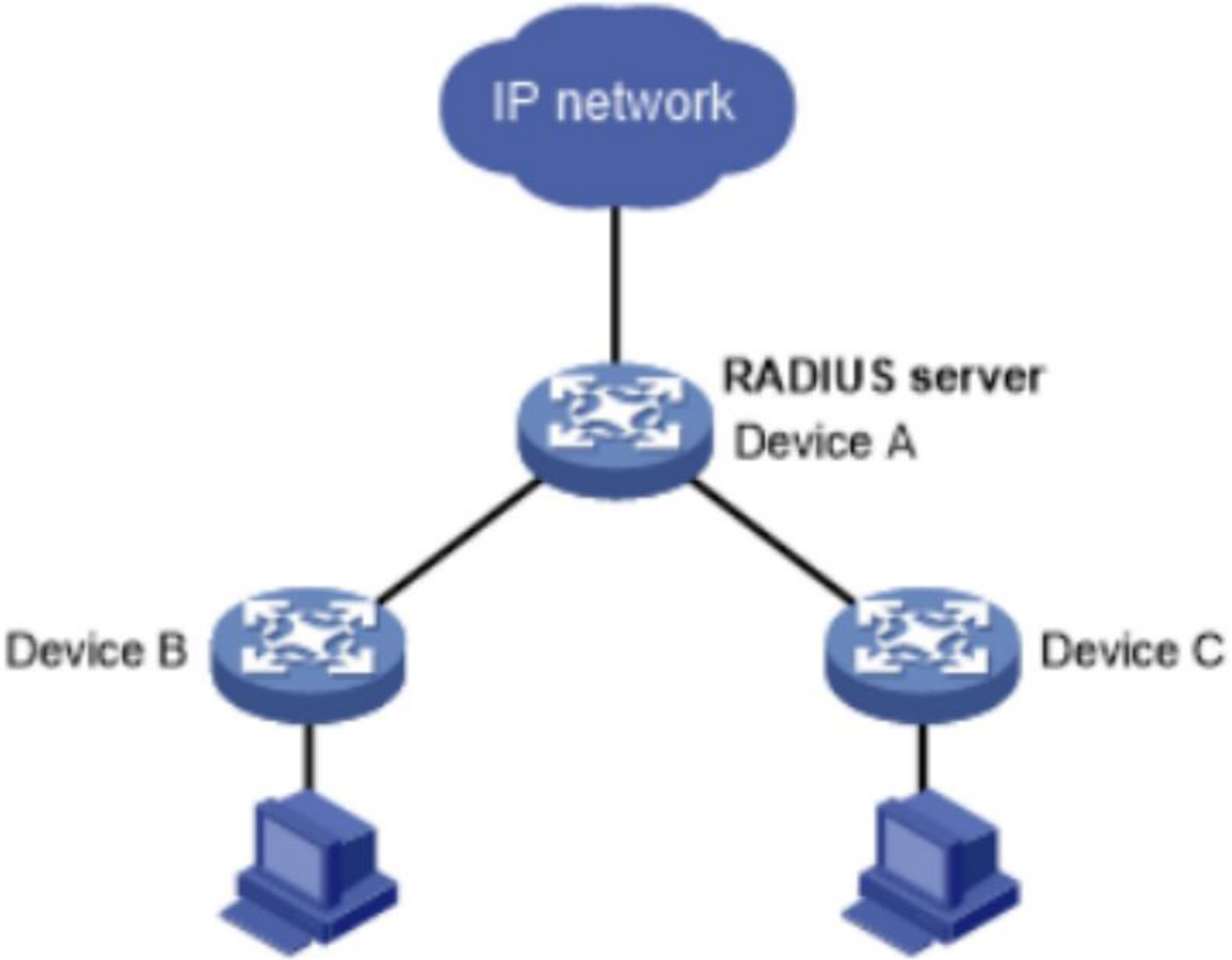
How its Works : A client (such as a Wi-Fi access point) sends user credentials to a RADIUS server, which authenticates and authorizes access.

**Key Features:**

Supports AAA (Authentication, Authorization, Accounting).

•Encrypts only the password, not the entire packet.

•UDP-based communication.


IP network
RADIUS server
Device A
Device B
Device C

# Network Protocols for Authentication

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

•Provides centralized authentication and access control for network devices (like routers, switches).

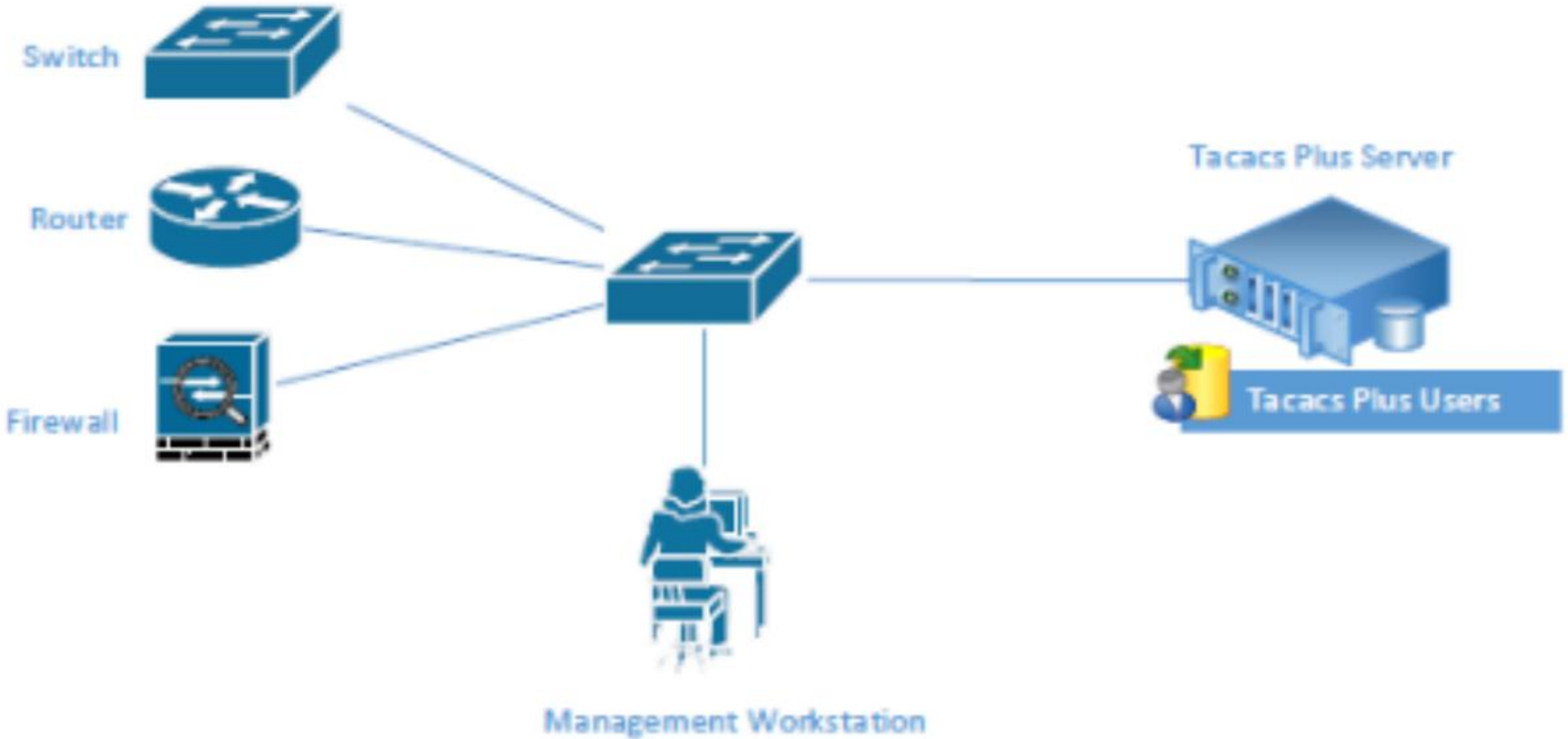
**How it Works:** Splits authentication, authorization, and accounting, allowing greater control over device access policies.

**Key Features:**

•Full packet encryption for enhanced security.

•TCP-based communication (more reliable than RADIUS)

•Flexible per-command authorization.


Switch
Router
Firewall
Tacacs Plus Server
Tacacs Plus Users
Management Workstation

# Network Protocols for Authentication

- LDAP (Lightweight Directory Access Protocol)

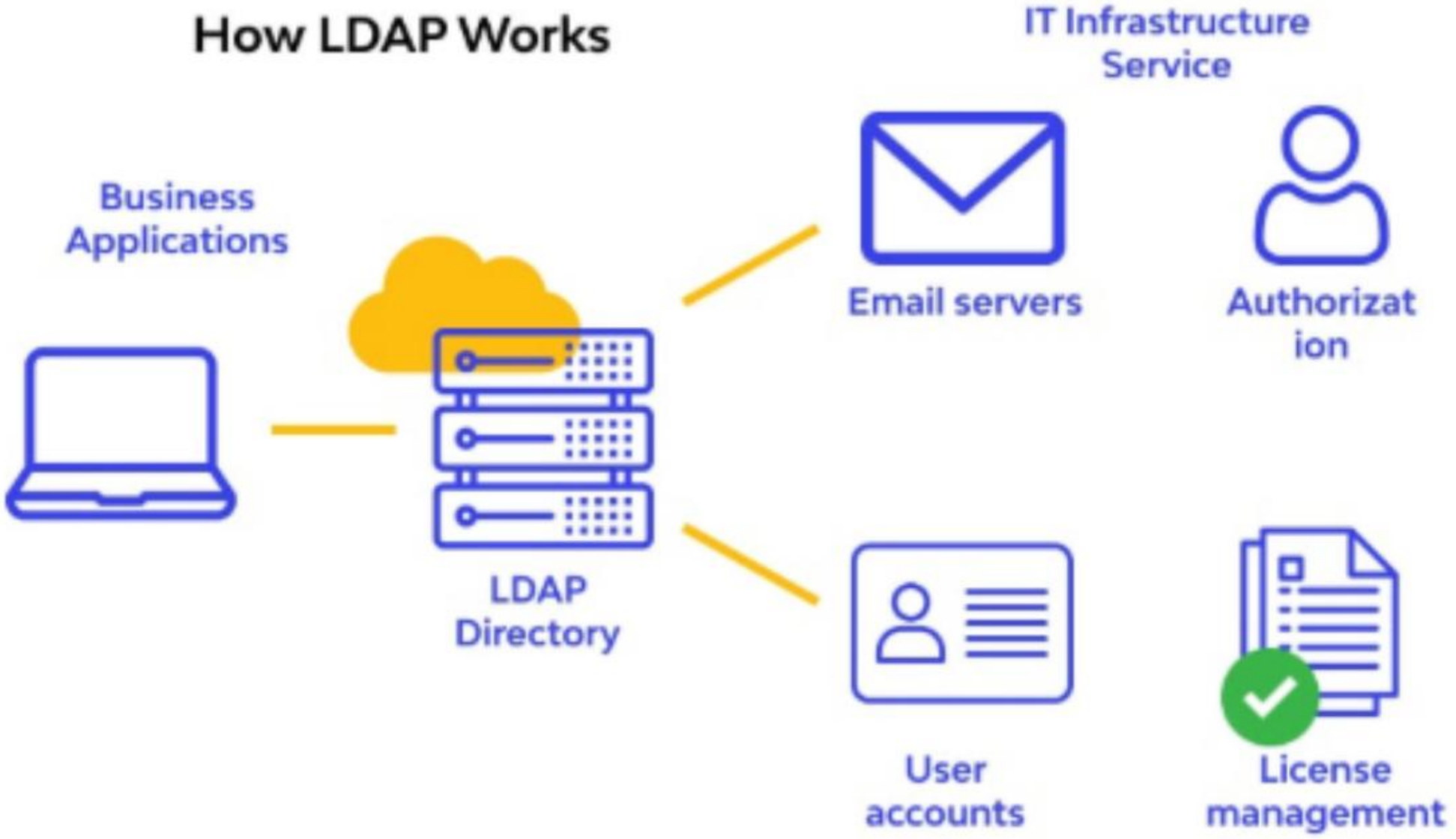
  Directory service protocol for accessing and managing directory information over a network. Commonly used to store user information and provide authentication.

  **How it Works:** Clients query an LDAP server to authenticate users or fetch directory information like usernames, email addresses, or permissions.

  **Key Features:**

- Works over TCP/UDP .
- Hierarchical structure (like a phone directory).
- Commonly integrated with Active Directory (AD).

# How LDAP Works



# Network Protocols for Authentication

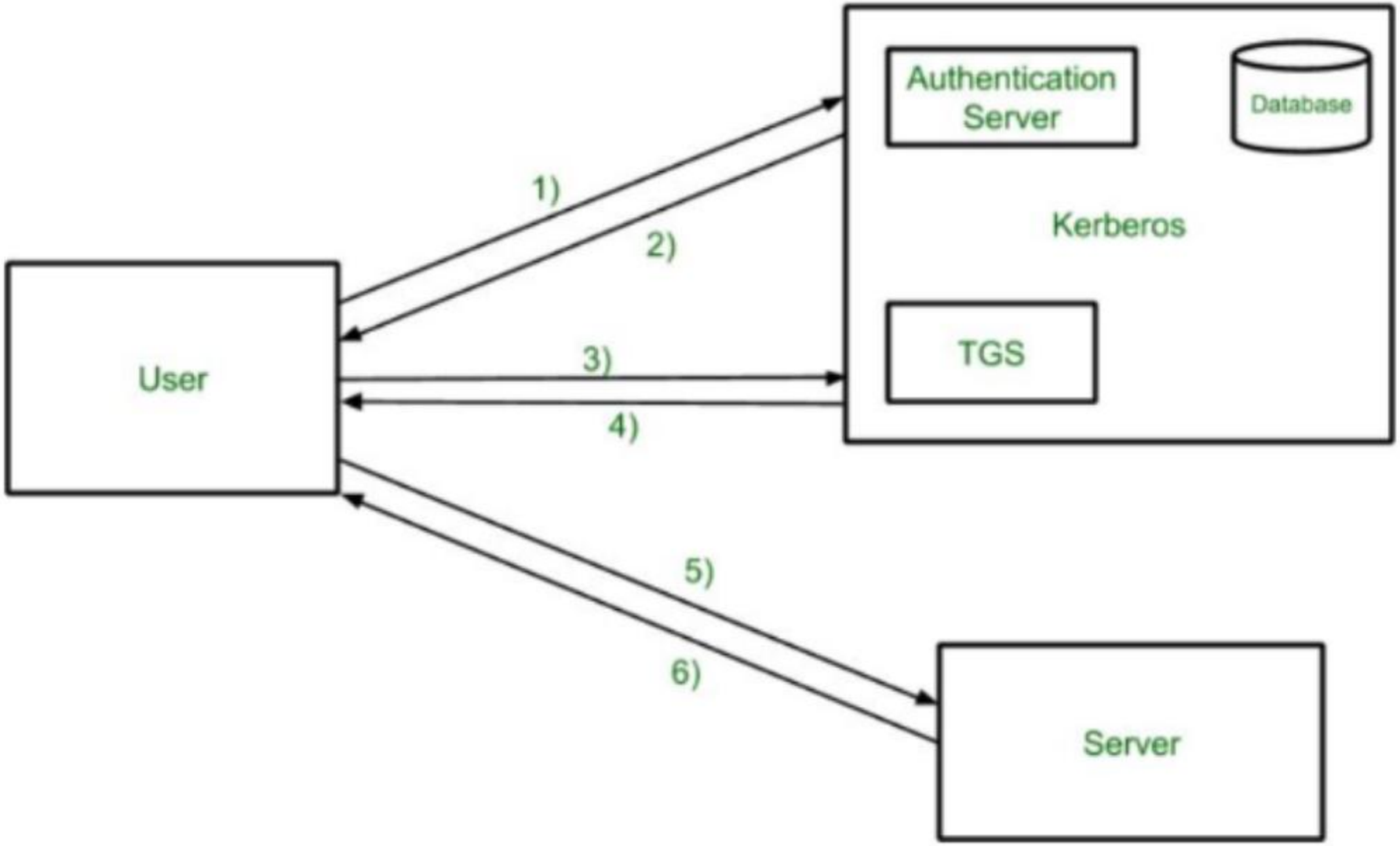
- Kerberos

  Secure authentication protocol using a ticketing system to prove user identity without repeatedly sending passwords.

  **How it Works:** The client authenticates with a Key Distribution Center (KDC) and receives a ticket-granting ticket (TGT)..

  **Key Features:**

- Prevents replay attacks.
- Widely used in enterprise environments.
- Strong cryptographic security.


Authentication Server
Database
Kerberos
TGS
User
1)
2)
3)
4)
5)
6)
Server

# Network Protocols for Authentication

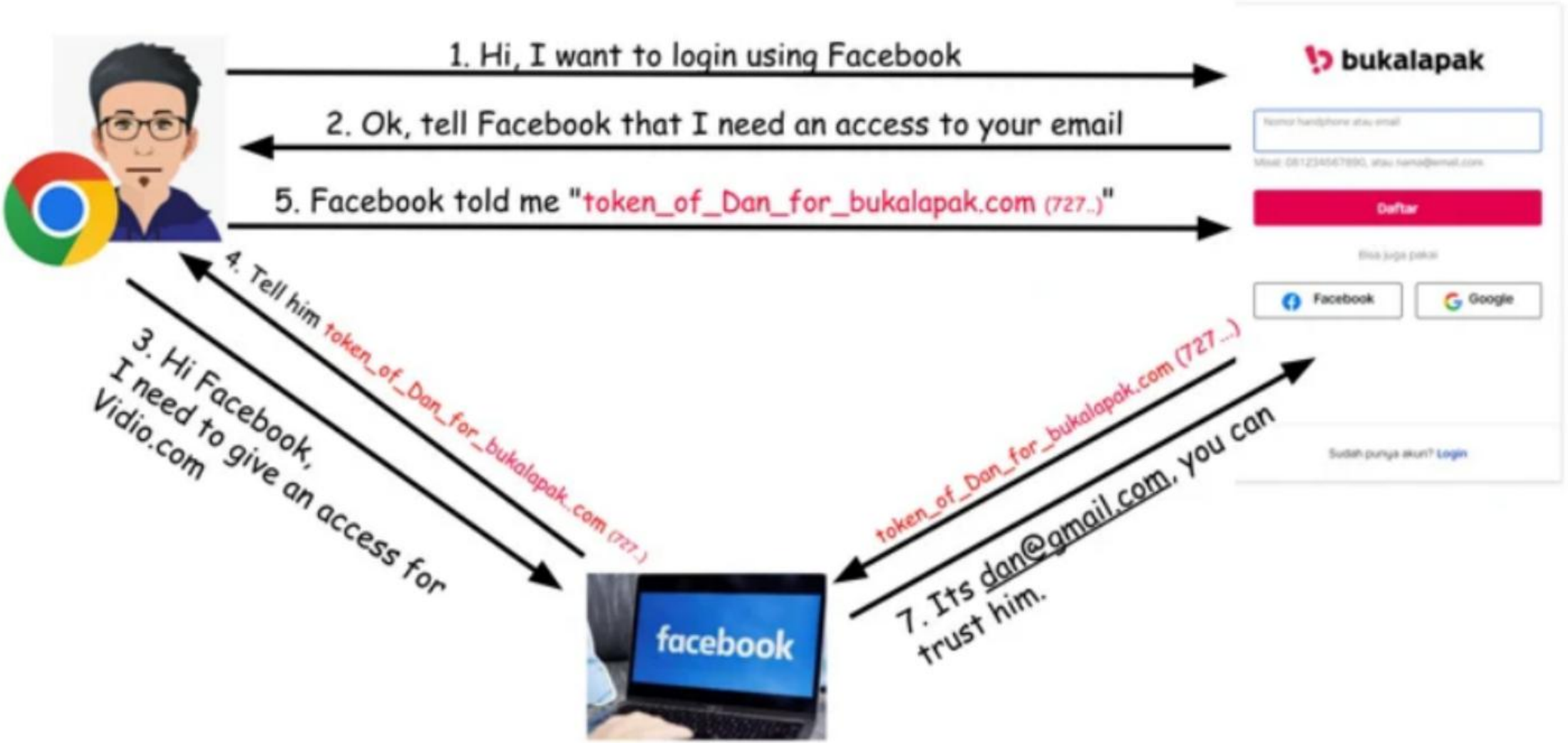
- OAuth (Open Authorization)

  Allows third-party applications limited access to user resources without sharing user credentials.

  **How it Works:** The user authorizes a third-party application via an authorization server, which issues access tokens to control resource access.

  **Key Features:**

- Token-based access management.
- Does not directly handle authentication.


1. Hi, I want to login using Facebook
2. Ok, tell Facebook that I need an access to your email
5. Facebook told me "token_of_Dan_for_bukalapak.com (727..)"
4. Tell him token_of_Dan_for_bukalapak.com (727..)
3. Hi Facebook, I need to give an access for Vidio.com
token_of_Dan_for_bukalapak.com (727...)
7. Its dan@gmail.com, you can trust him.
bukalapak
Daftar
Facebook
Google
facebook

# Secure Authentication Protocols

- Secure Socket Layer (SSL) and Transport Layer Security (TLS)

  Cryptographic protocols that secure communication over networks

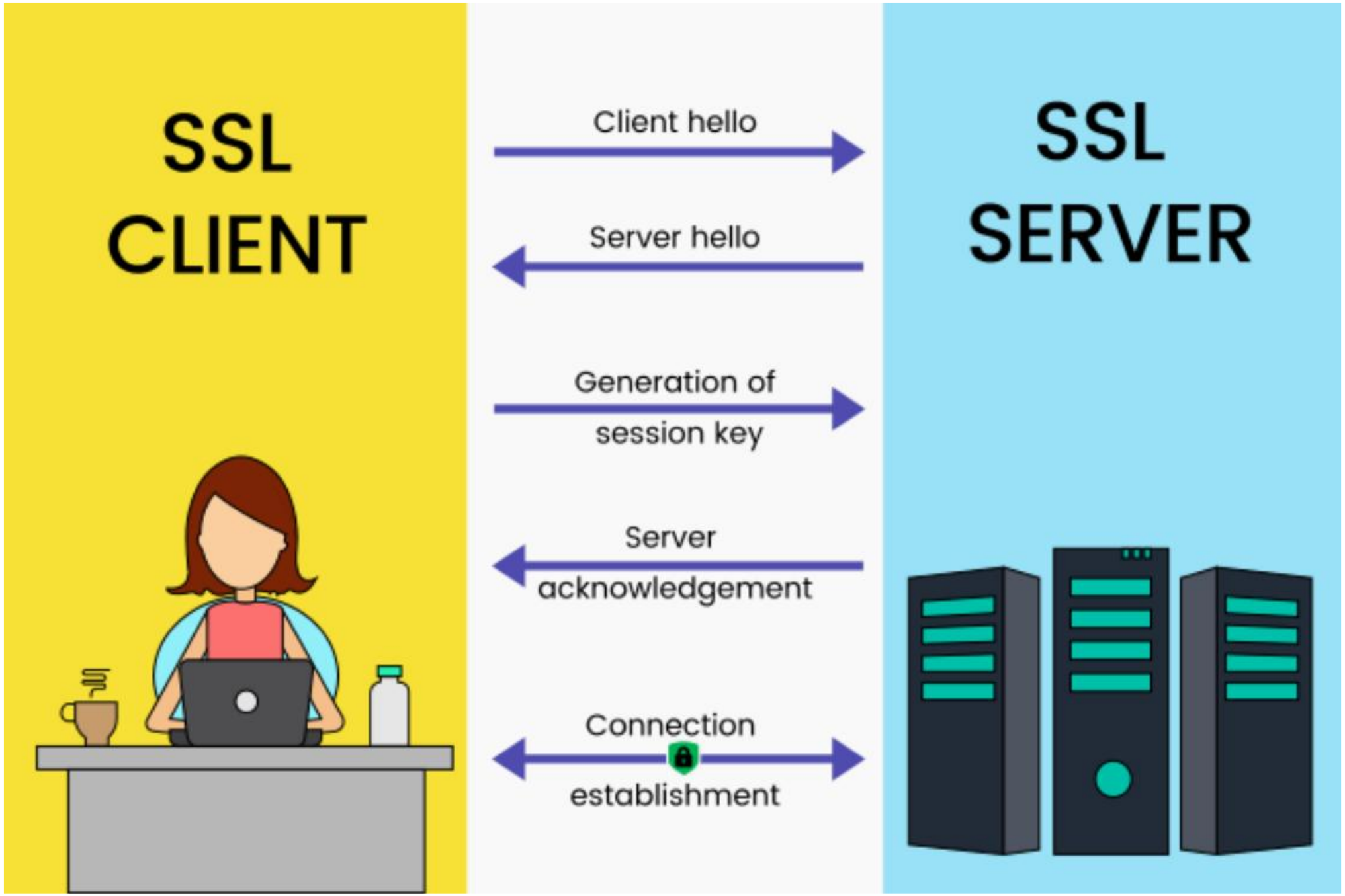
  **How it Works:** Handshake Process.

  **Key Features:**

Symmetric and asymmetric encryption.

Certificate-based authentication.

Integrity via message authentication codes.


SSL
CLIENT
Client hello
Server hello
Generation of
session key
Server
acknowledgement
Connection
establishment
SSL
SERVER

# Secure Authentication Protocols

- Secure Shell (SSH)

  Protocol for secure remote access and file transfers

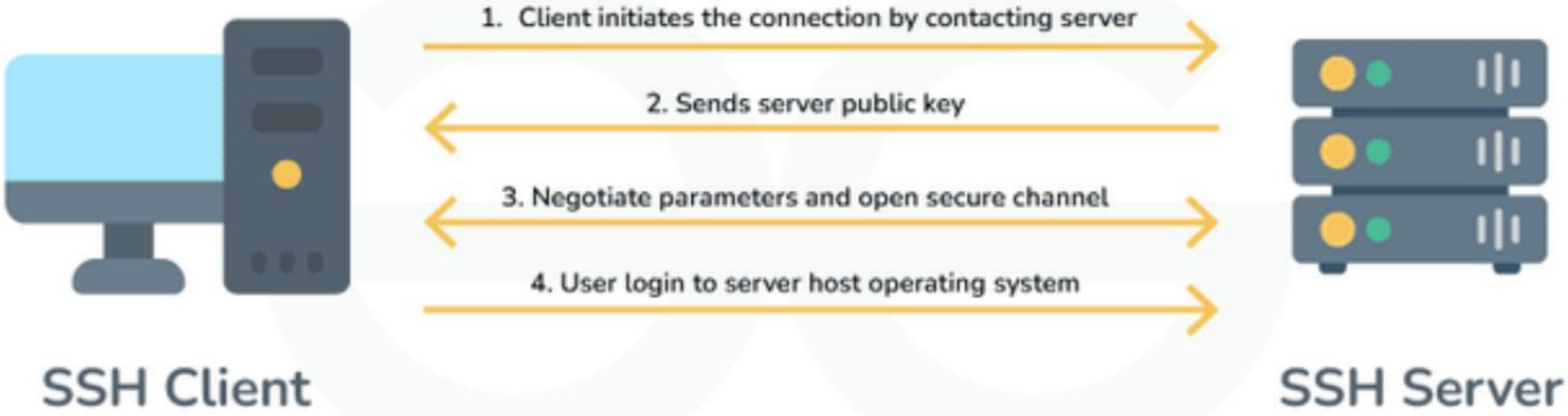
- **How it Works:** Key Exchange: Secure exchange of session keys, Authentication: Using public/private keys or passwords, Encrypted Communication: Protecting transmitted data

  **Key Features:**

Public-key cryptography

Secure tunneling

Authentication using passwords or keys


1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system
SSH Client
SSH Server


# Secure Authentication Protocols

- Extensible Authentication Protocol (EAP)

  protocol that allows for multiple authentication methods to be used for network access

  **How it Works:**

  EAP specifies the structure of the communication between a client and an authentication server.

- EAP supports a variety of authentication methods, including passwords, certificates, smart cards, and one-time passwords.

# Secure Authentication Protocols

## *Extensible Authentication Protocol (EAP)*

**Key Features of EAP:**

**1.Extensibility**: EAP supports various authentication methods, such as passwords, certificates, smart cards, tokens, and biometrics.

**2.Layer Independence**: EAP can be implemented over different layers, including wireless (IEEE 802.1X) and wired networks.

**3.Scalability**: It is suitable for enterprise-level environments with a large number of users and devices.

**Applications of EAP:**

- **Wi-Fi Security**: Often implemented with IEEE 802.1X in enterprise wireless networks.
- **VPNs and Remote Access**: Used for secure user authentication in remote connections.
- **Network Access Control (NAC)**: Ensures that only authenticated and authorized devices can connect.

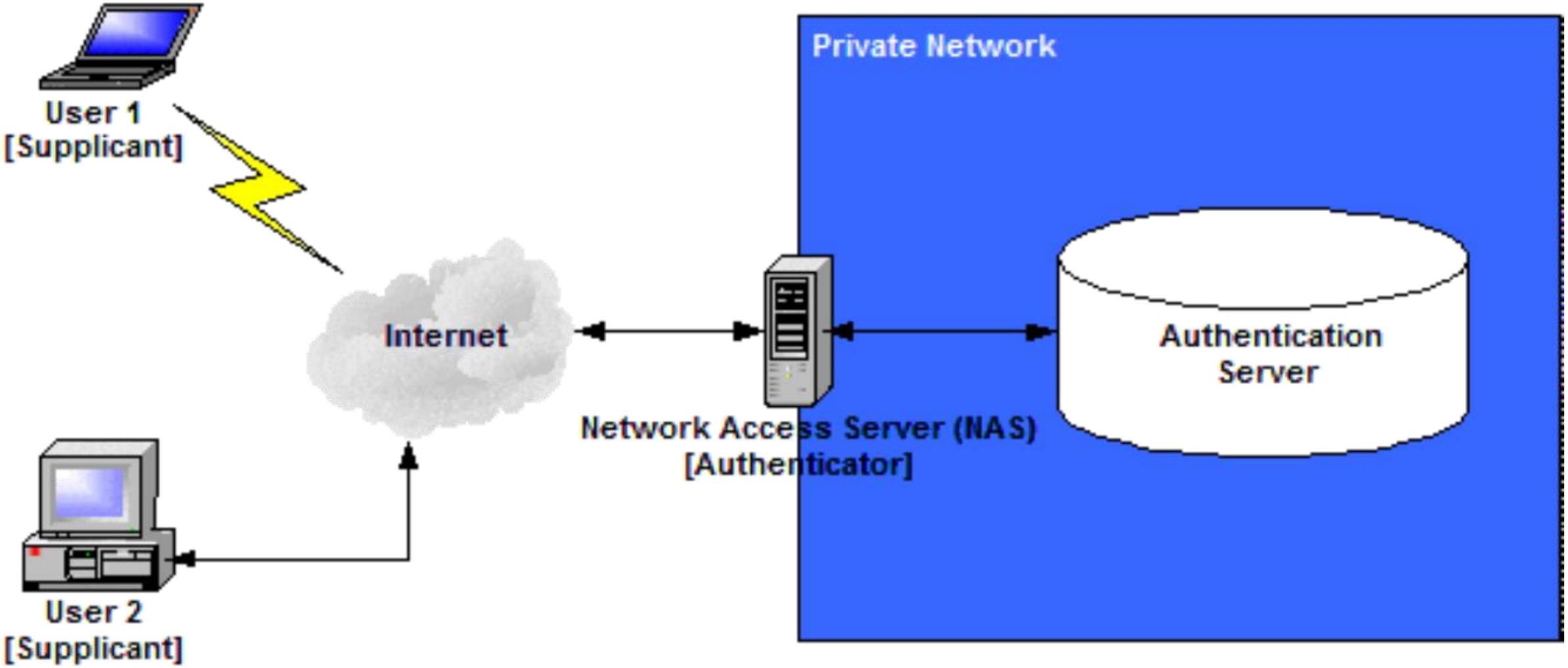



Figure 1: EAP Architecture

# Secure Authentication Protocols

- *OpenID Connect*

  OpenID Connect is an identity layer built on top of OAuth 2.0. While OAuth 2.0 is about authorization, OIDC is about authentication—verifying who the user is.

  **How it Works:**

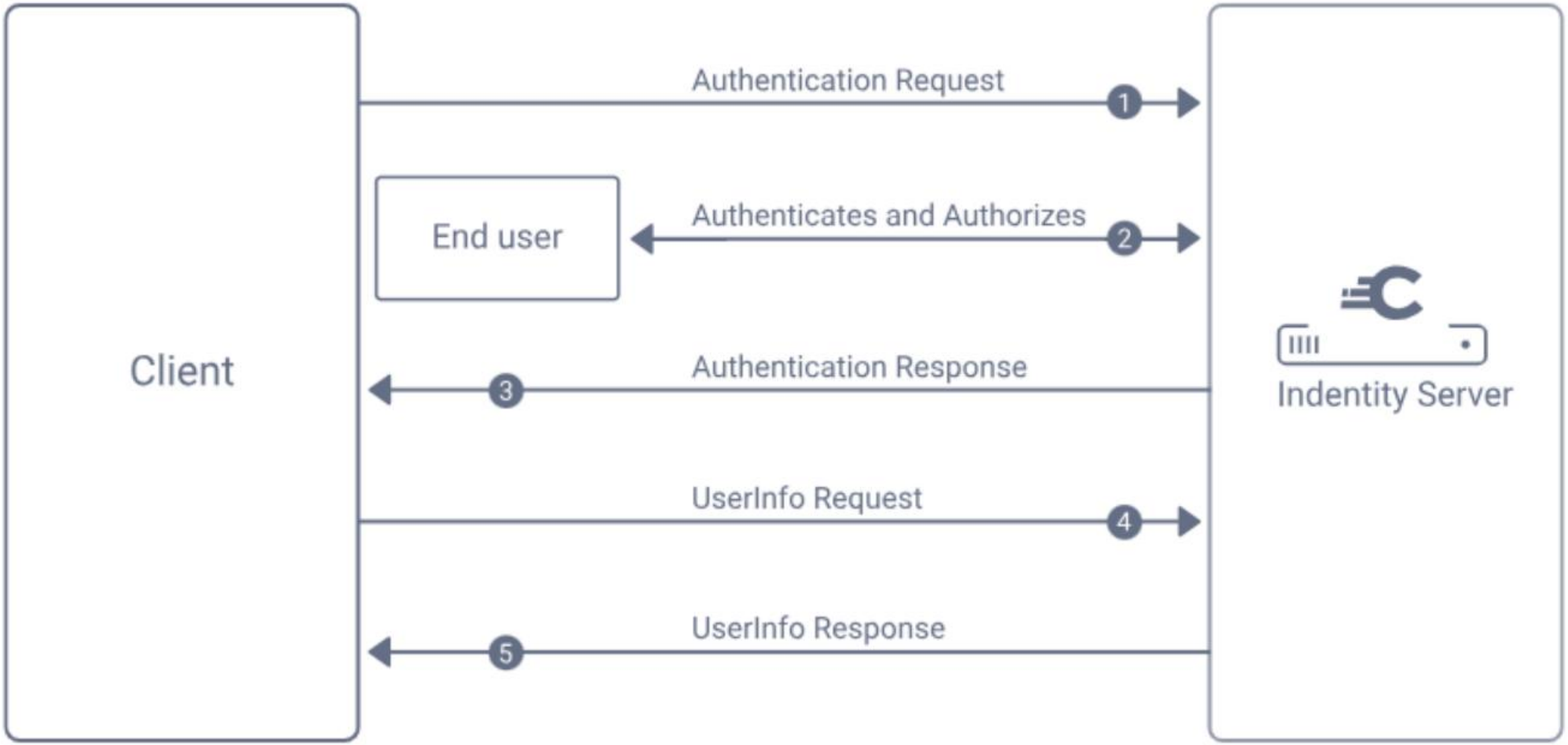
  *OpenID Connect (OIDC) works by* allowing users to log into different applications using a single set of credentials from a trusted identity provider.

# Secure Authentication Protocols

## OpenID Connect

**Key Features of OpenID Connect:**

1. **User Authentication**: Confirms the user's identity and provides basic profile information.
2. **Token Types**:
    1. **ID Token**: A JSON Web Token (JWT) containing user identity claims.
    2. **Access Token**: Used for resource access (inherited from OAuth 2.0).
    3. **Standardized User Info**: Provides a user info endpoint for fetching profile details.


Client
End user
Authentication Request
1
Authenticates and Authorizes
2
Authentication Response
3
UserInfo Request
4
UserInfo Response
5
Indentity Server