

N|DE
Network Defense Essentials

Module 01

Network Security Fundamentals



Module Objectives

1. Understanding the Goals of Network Defense
2. Understanding Information Assurance (IA) Principles
3. Understanding the Benefits and Challenges of Network Defense
4. Overview of Different Types of Network Defense Approaches
5. Understanding the Different Types of Network Security Controls
6. Understanding the Different Network Security Protocols



Module Flow

01 **Understand Fundamentals of Network Security**

02 **Discuss Essential Network Security Protocols**

Essentials of Network Security

- A completely secure and robust network can be designed with proper **implementation** and **configuration** of network security elements

Elements of Network Security

- **Network Security Controls**
- **Network Security Protocols**
- **Network Security Devices**



Goal of Network Defense

The ultimate goal of network defense is to protect an organization's information, systems, and network infrastructure from **unauthorized access**, **misuse**, **modification**, **service denial**, or any **degradation** and **disruptions**

Organizations rely on **information assurance (IA) principles** to attain defense-in-depth security

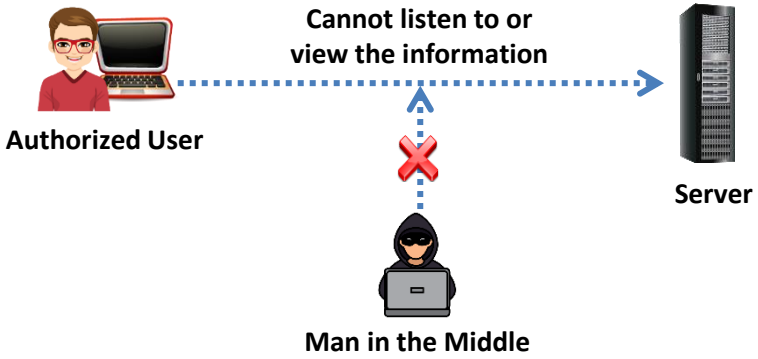
Information Assurance (IA) principles act as **enablers** for an organization's security activities to protect and defend the organizational network from security attacks

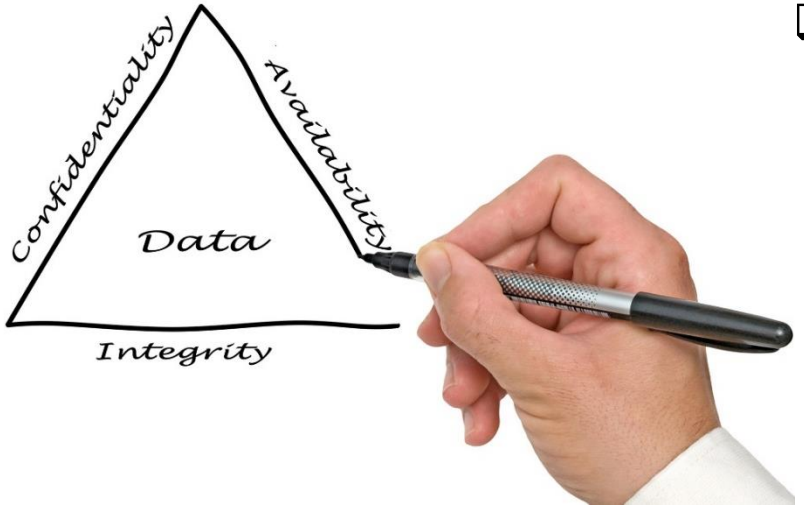


Information Assurance (IA) Principles

Confidentiality

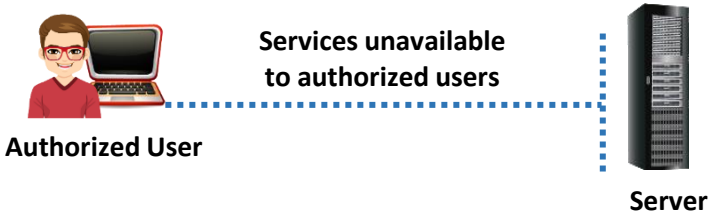
- Ensures information is not **disclosed** to unauthorized parties





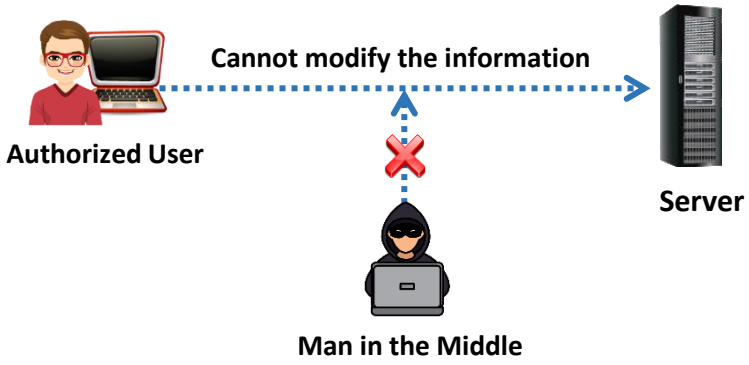
Availability

- Ensures information is **available** to authorized parties without any disruption



Integrity

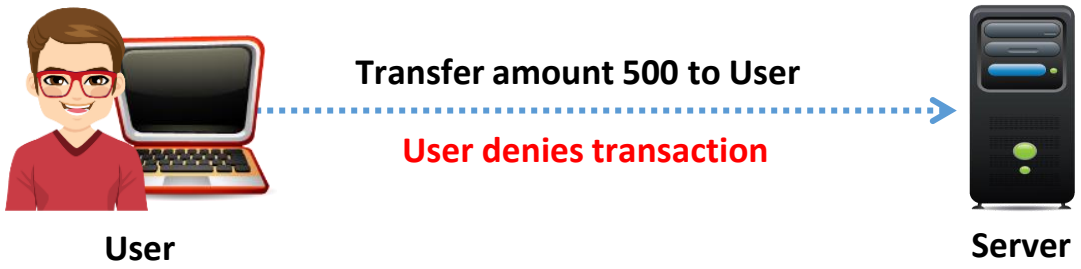
- Ensures information is not **modified** or **tampered** with by unauthorized parties



Information Assurance (IA) Principles (Cont'd)

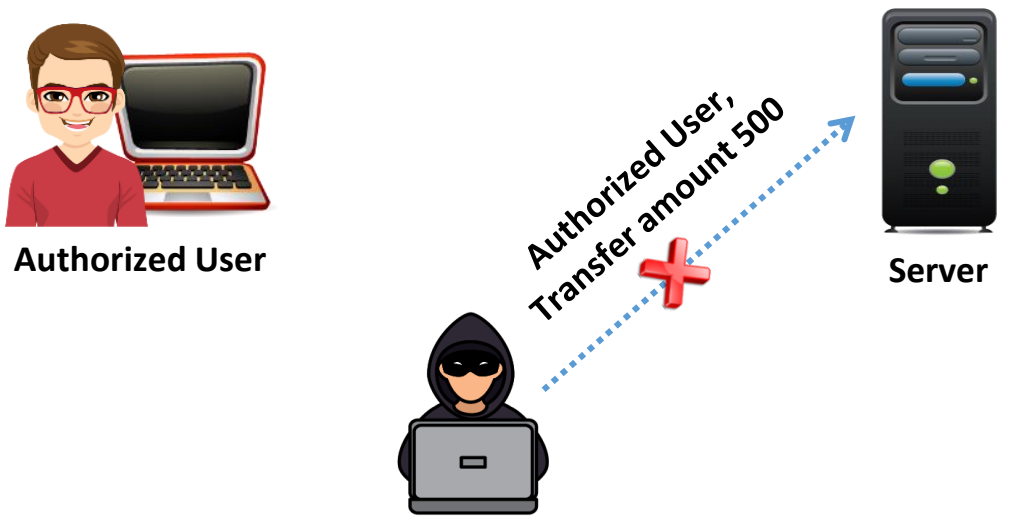
Non-repudiation

- Ensures that a party in a communication cannot deny **sending** the message



Authentication

- Ensures the **identity** of an individual is verified by the system or service





Network Defense Benefits

- **Protect** information assets
- **Comply** with government and industry specific regulations
- **Ensure** secure communication with clients and suppliers
- **Reduce** the risk of being attacked
- **Gain** competitive edge over competitor by providing more secure services

Network Defense Challenges

Distributed Computing Environments

- With the advancement in **modern technology** and to meet business requirements, networks are becoming **vast** and **complex**, potentially leading to serious **security vulnerabilities**. Attackers exploit exposed security vulnerabilities to compromise network security

Emerging Threats

- Potential threats to the network evolve each day. Network security attacks are becoming technically more **sophisticated** and **better organized**



Lack of Network Security Skills

- Organizations are failing to defend themselves against rapidly increasing network attacks due to the **lack of network security skills**



Types of Network Defense Approaches

Preventive Approaches

Consist of methods or techniques that are used to avoid threats or attacks on the target network

Retrospective Approaches

Consist of methods or techniques that examine the causes for attacks, and contain, remediate, eradicate, and recover from damage caused by the attack on the target network



Reactive Approaches

Consist of methods or techniques that are used to detect attacks on the target network

Proactive Approaches

Consist of methods or techniques that are used to make informed decisions on potential attacks in the future on the target network

Network Security Controls: Administrative Security Controls

- The management implements administrative access controls to **ensure** the **safety** of the organization

Examples of Administrative Security Controls

01 Regulatory framework Compliance

02 Security policy

03 Employee Monitoring and Supervising

04 Information Classification

05 Security Awareness and Training

Network Security Controls: Physical Security Controls

- This is a set of security measures taken to **prevent unauthorized access** to physical devices

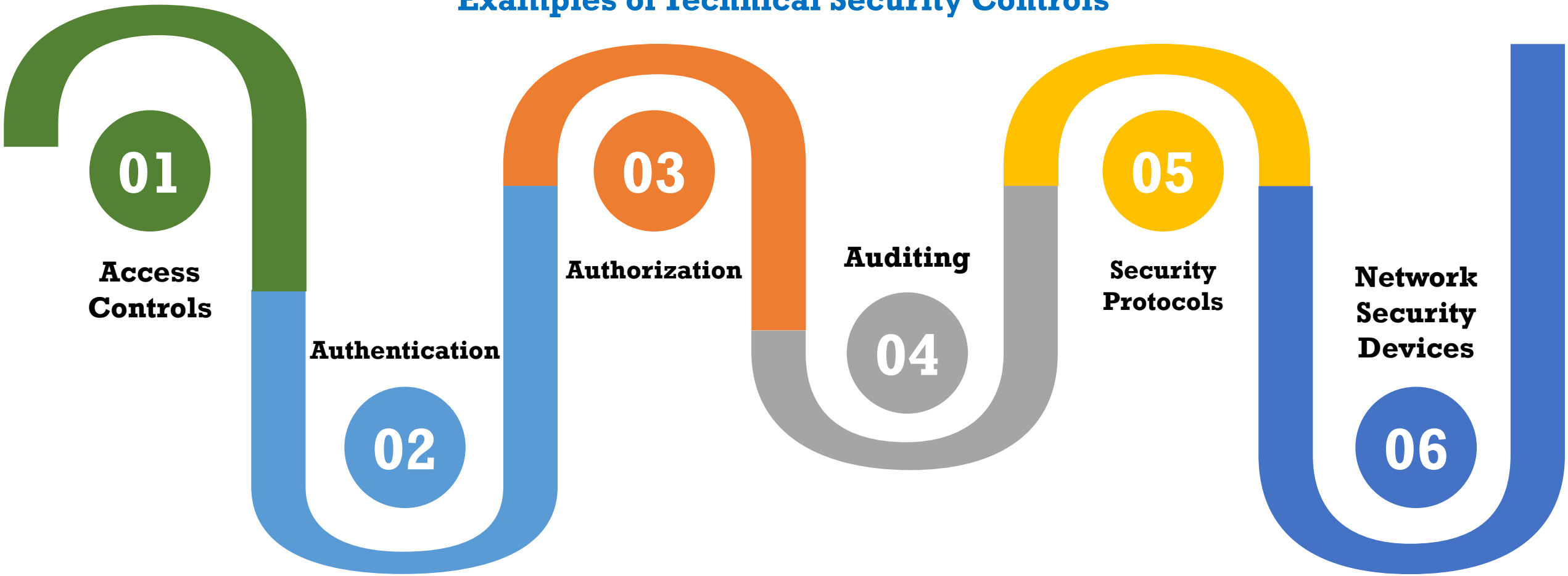
Examples of Physical Access Controls

 **Locks**	 **Fences**	 **Badge system**	 **Security guards**	 **Mantrap doors**
 **Biometric system**	 **Lighting**	 **Motion detectors**	 **Closed-circuit TVs**	 **Alarms**

Network Security Controls: Technical Security Controls

- This is a set of security measures taken to protect data and systems from unauthorized personnel

Examples of Technical Security Controls





Module Flow

01 Understand Fundamentals of Network Security

02 Discuss Essential Network Security Protocols

Network Security Protocols

- RADIUS
- TACACS+
- Kerberos
- PGP
- S/MIME



- Secure HTTP
- HTTPS
- TLS
- SSL
- IPsec

Remote Authentication Dial-in User Service (RADIUS)

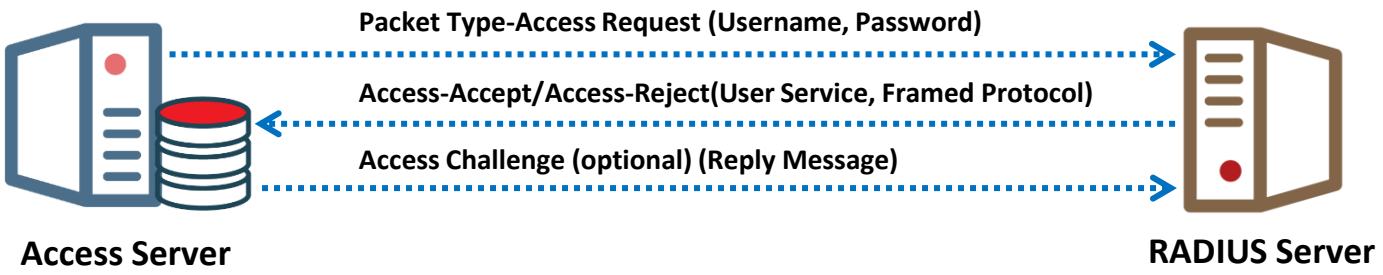
- Remote authentication dial-in user service (RADIUS) is an **authentication protocol** which provides centralized authentication, authorization, and accounting (AAA) for remote access servers to communicate with a central server

Authentication Steps in RADIUS

1) A client initiates a connection by sending the **access-request packet** to the server

2) The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **access-accept message** along with the **access-challenge** to the client for additional authentication, else it sends back an **accept-reject** message

3) Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted

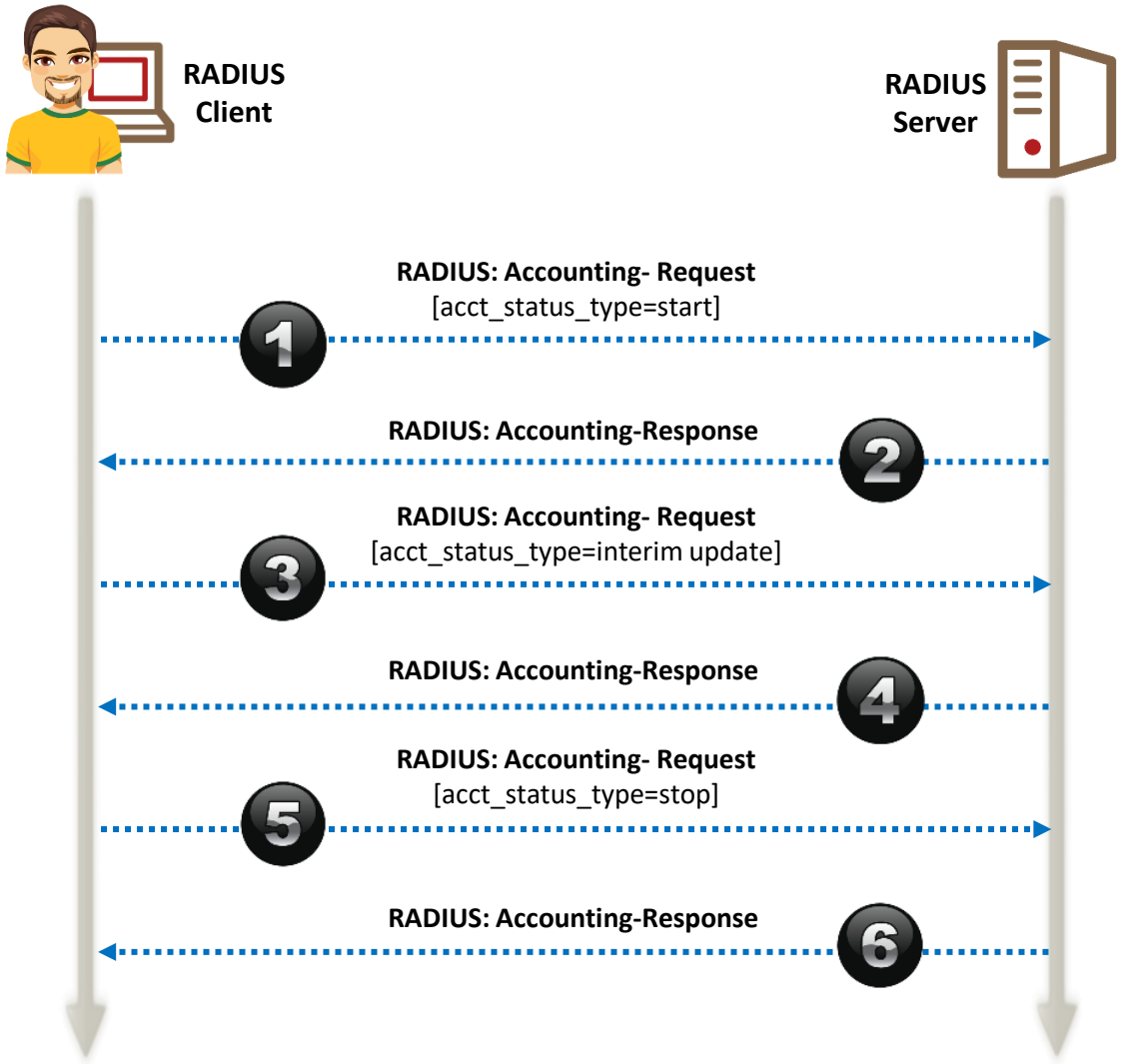


Remote Authentication Dial-in User Service (RADIUS) (Cont'd)

Radius Accounting Steps

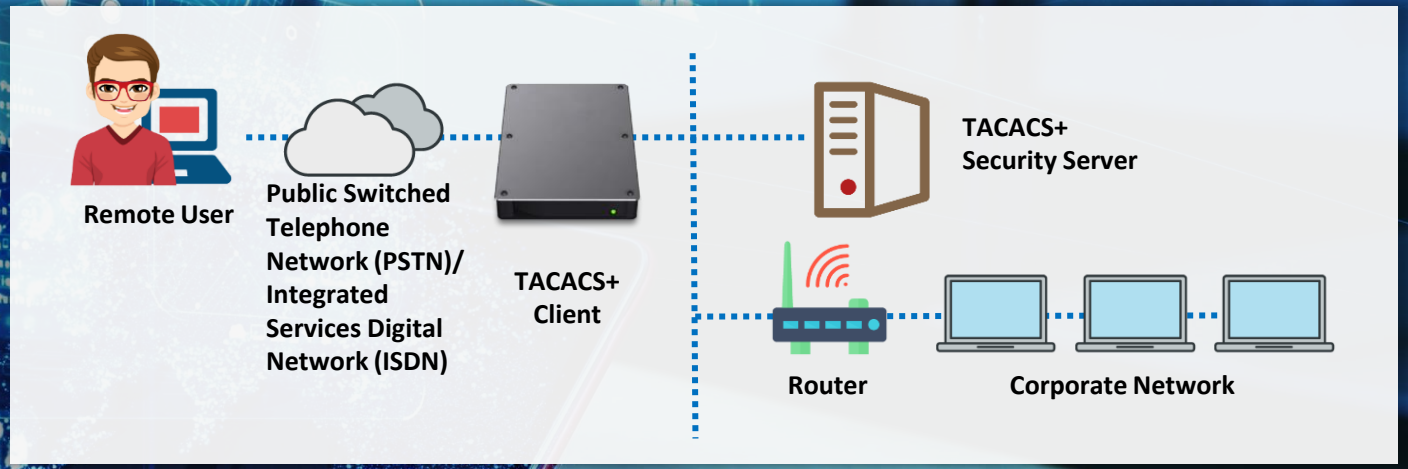
- Client sends the **accounting-request** to the server to specify the accounting information for a connection that was accepted

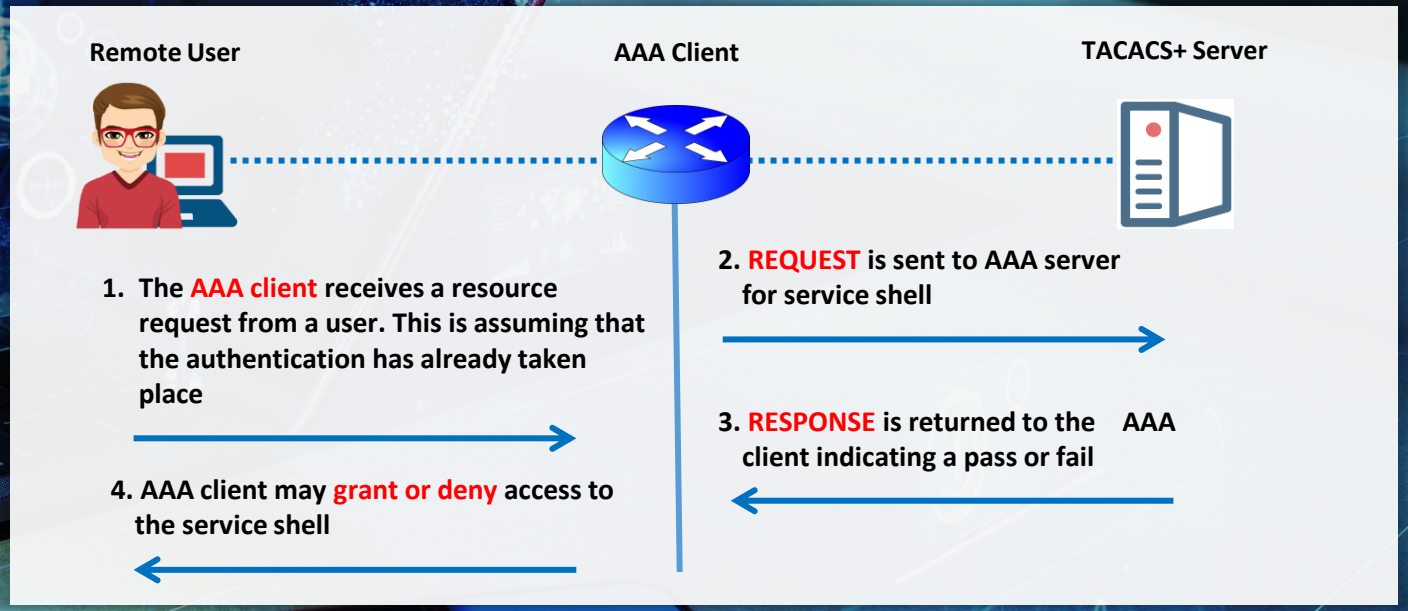
- The server receives this message and sends back the **accounting-response message** which states the successful establishment of the network



Terminal Access Controller Access Control System Plus (TACACS+)

- The terminal access controller access control system plus (TACACS+) is a **network security protocol** used for AAA of network devices such as switches, routers, and firewalls through one or more **centralized servers**
- TACACS+ **encrypts** the entire communication between the client and the server including the user's password which protects it from sniffing attacks
- It is a **client-server model** approach where the client (user or network device) requests for connection to a server, the server authenticates the user by examining their credentials





Kerberos

- Kerberos is an **authenticating method** for accessing a network

Kerberos authentication protocol (KAP)

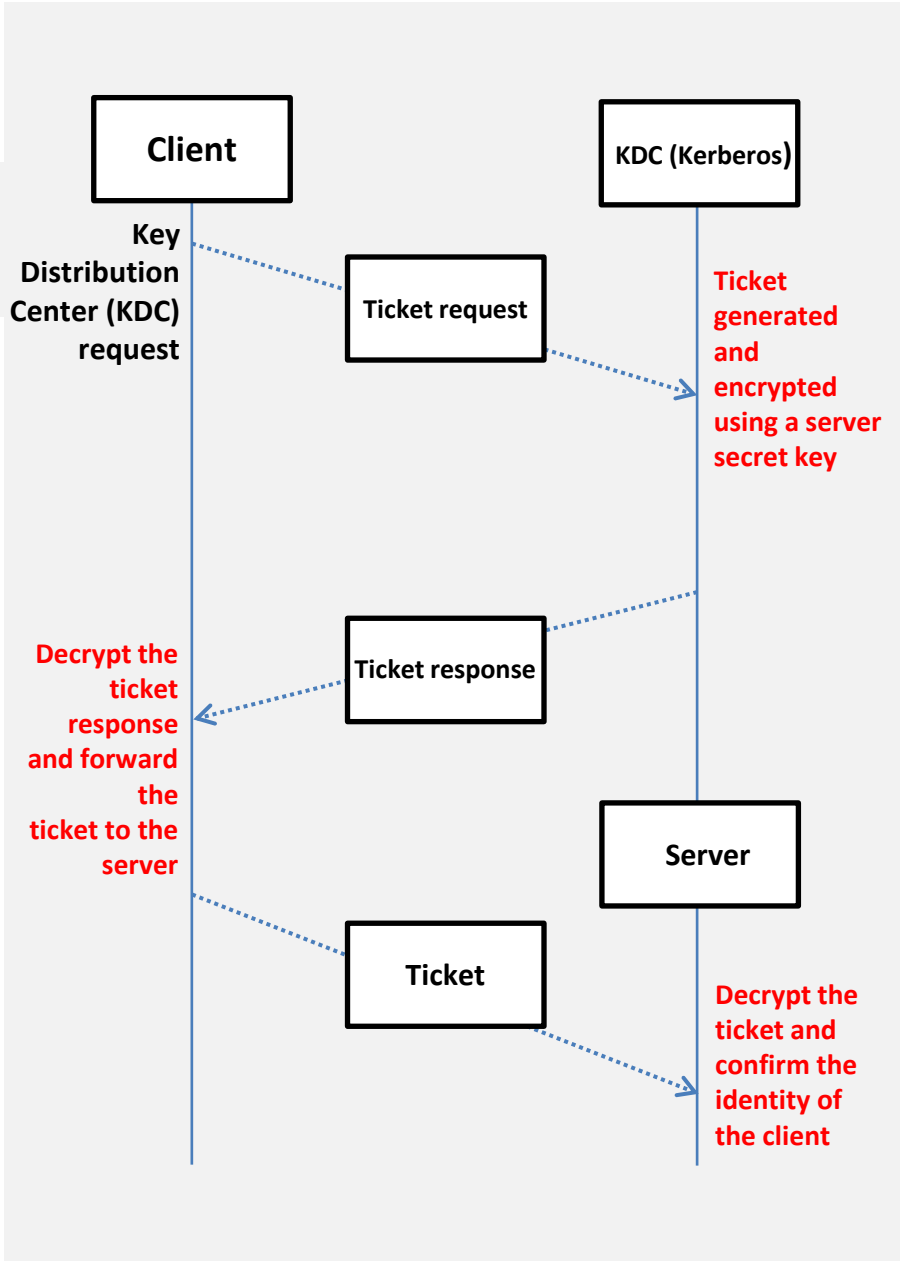
01 A user sends his/her credentials to an **authentication server** (**AS**)

02 The AS hashes the password of the user and verifies their credentials in the active directory database. If the credential matches, then AS (consisting of the ticket granting service, TGS) sends back the TGS session key and ticket granting ticket (TGT) to the user to create a session

03 Once users are authenticated, they send the TGT to request a service ticket to the server or TGS for accessing the services

04 The TGS authenticates the TGT and grants a **service ticket** to the user. The service ticket consists of the ticket and a session key

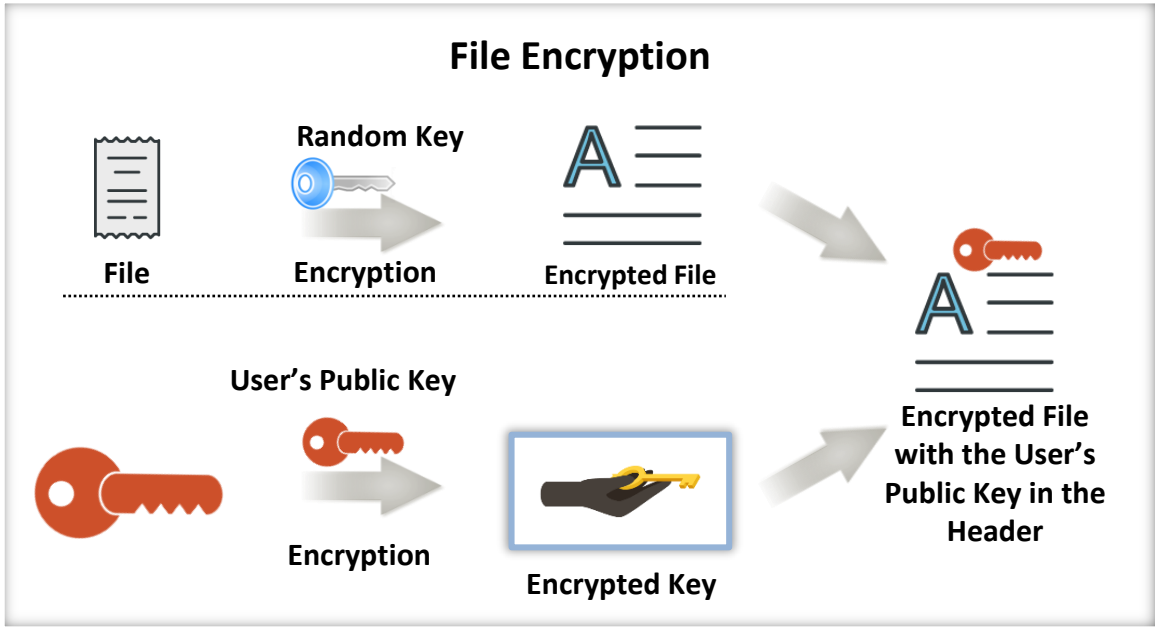
05 The client sends the service ticket to the server. The server uses its key to **decrypt** the information from the TGS and the client is authenticated to the server

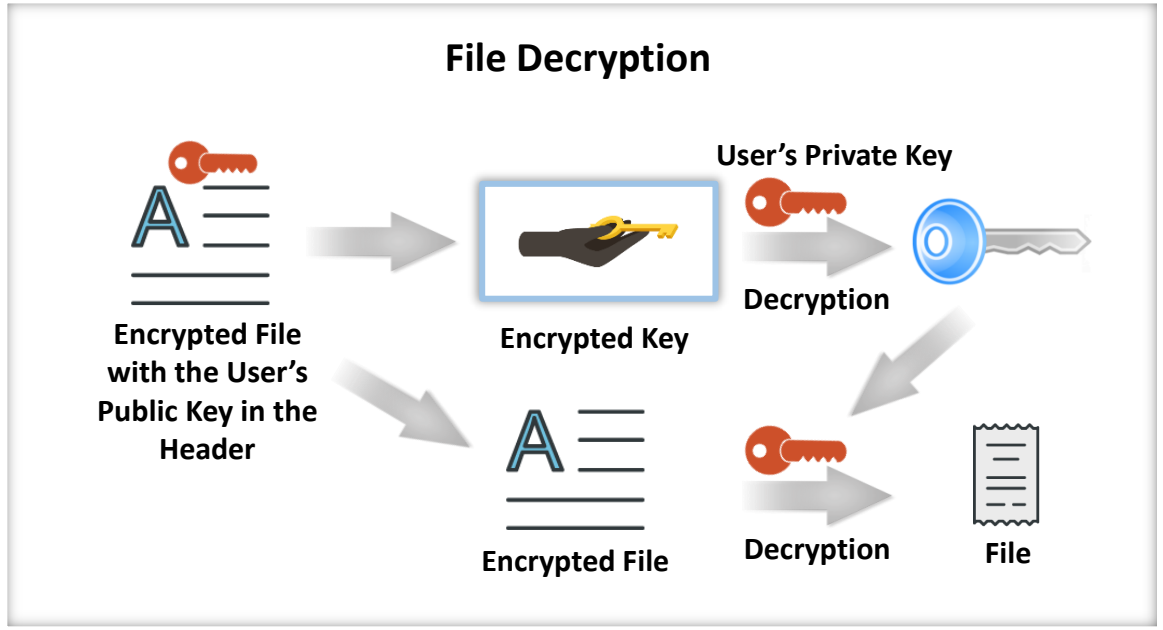


Pretty Good Privacy (PGP)

- Pretty good privacy (PGP) is an application layer protocol which provides **cryptographic privacy** and authentication for network communication

- It encrypts and decrypts email communication as well as authenticates messages with **digital signatures** and encrypts stored files



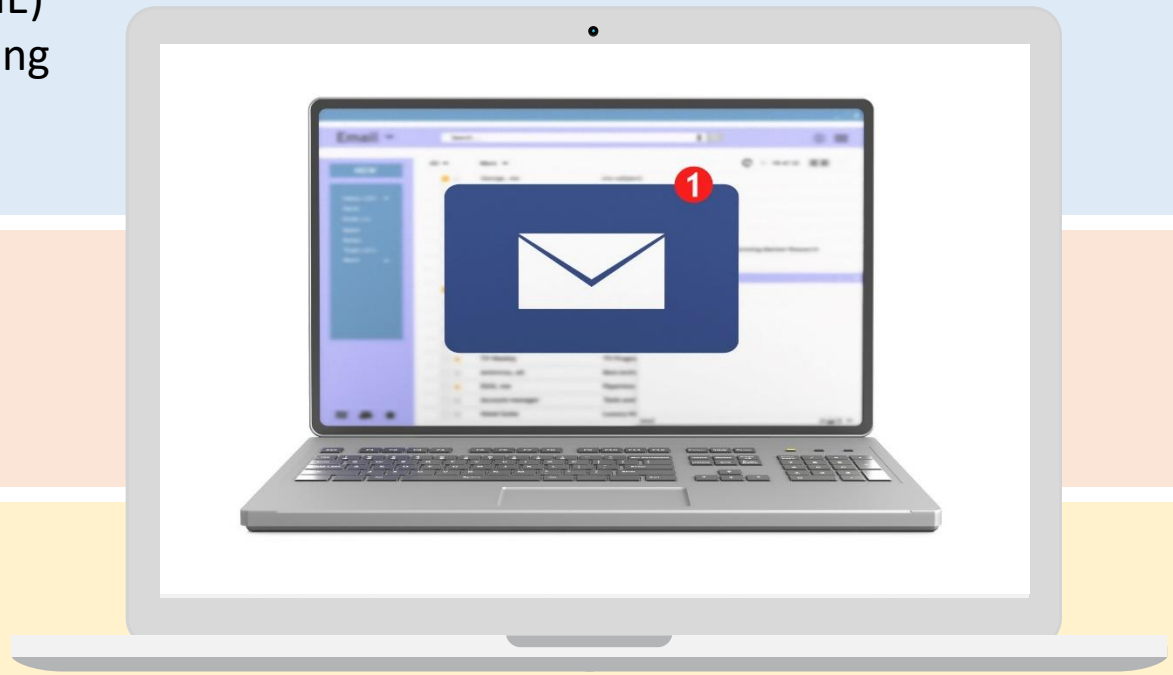


Secure/Multipurpose Internet Mail Extensions (S/MIME)

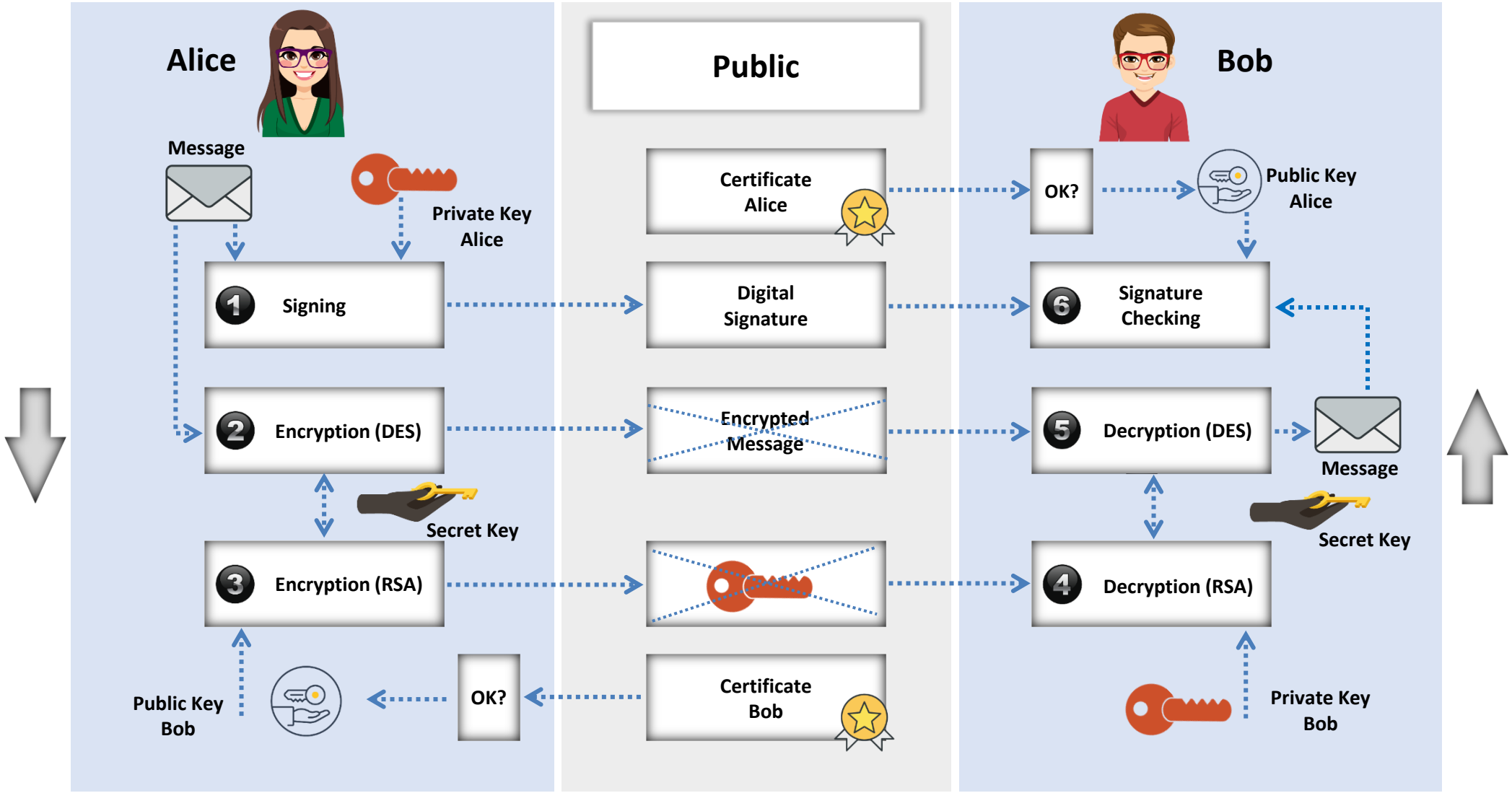
01 > Secure/multipurpose internet mail extensions (S/MIME) is an application layer protocol which is used for sending **digitally signed** and **encrypted email messages**

02 > It uses the **RSA** system for email encryption

03 > Network defenders need to **enable** S/MIME-based security for mailboxes in their organizations

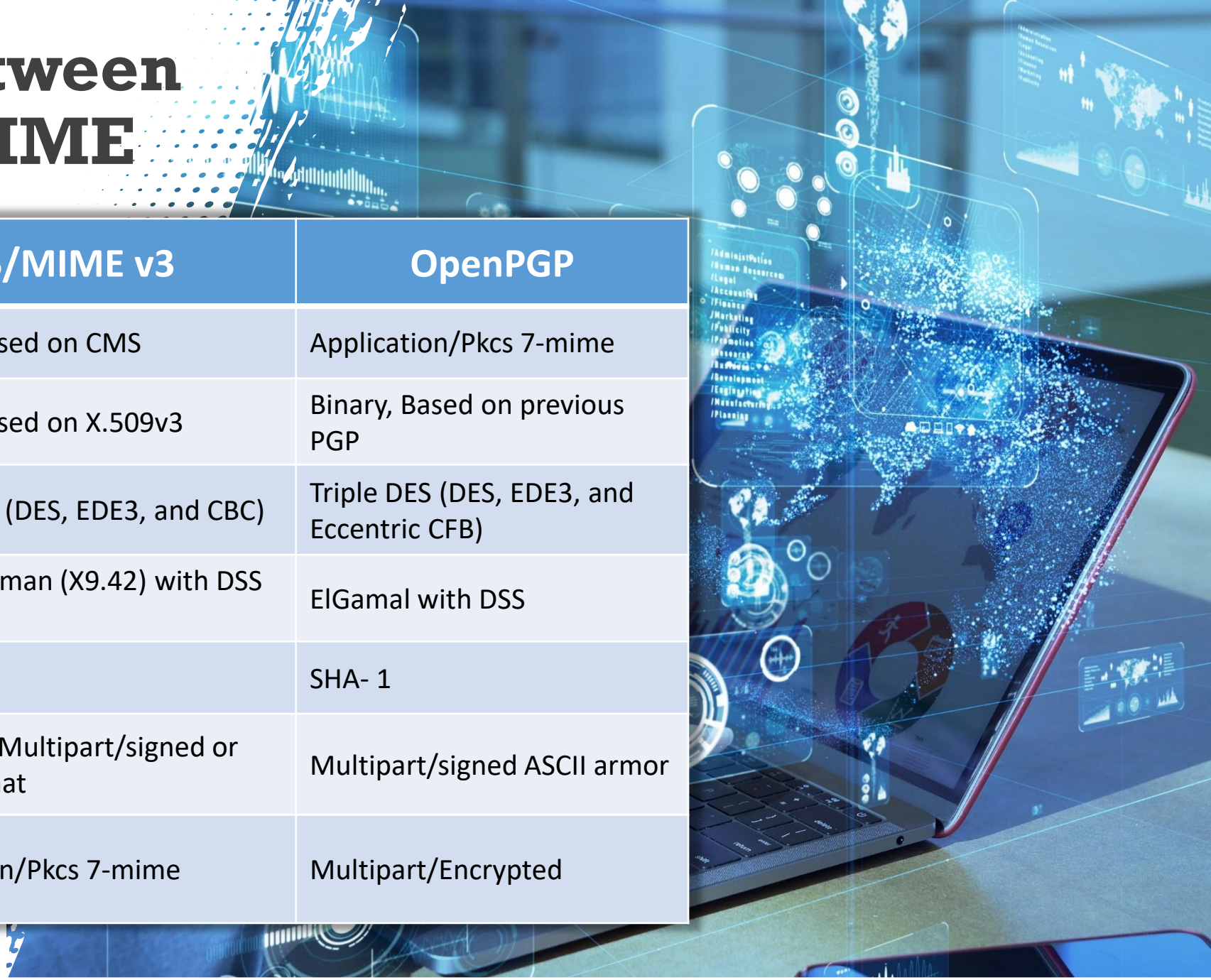


Secure/Multipurpose Internet Mail Extensions (S/MIME) (Cont'd)



Differences between PGP and S/MIME

Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, and CBC)	Triple DES (DES, EDE3, and Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

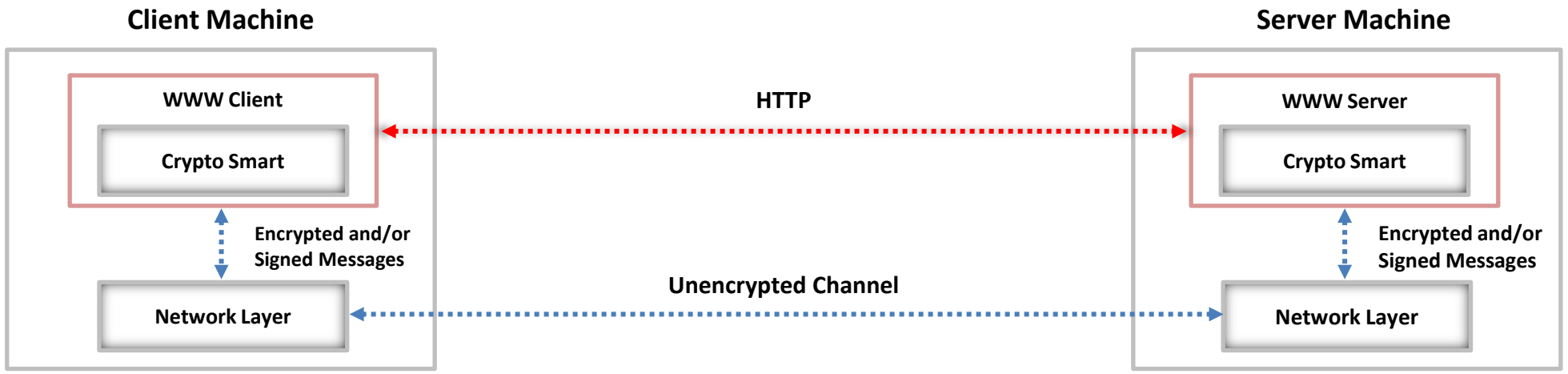


Secure Hypertext Transfer Protocol (S-HTTP)



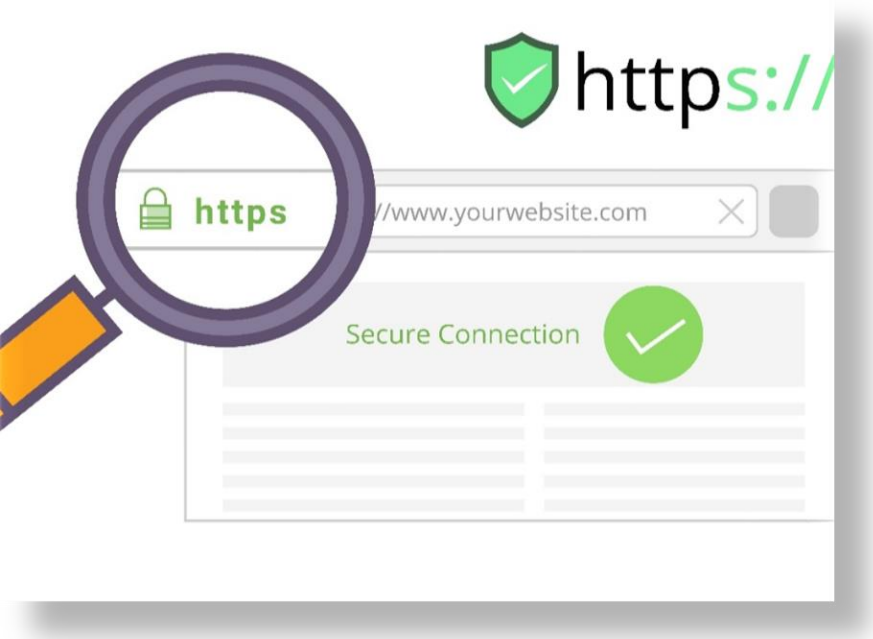
- Secure hypertext transfer protocol (S-HTTP) is an application layer protocol that is used to **encrypt web communications** carried over HTTP
- It is an alternative for the **HTTPS** (SSL) protocol
- It ensures **secure data transmission** of individual messages, while SSL establishes a secure connection between two entities thus ensuring security of the entire communication

S-HTTP Application- Level Security

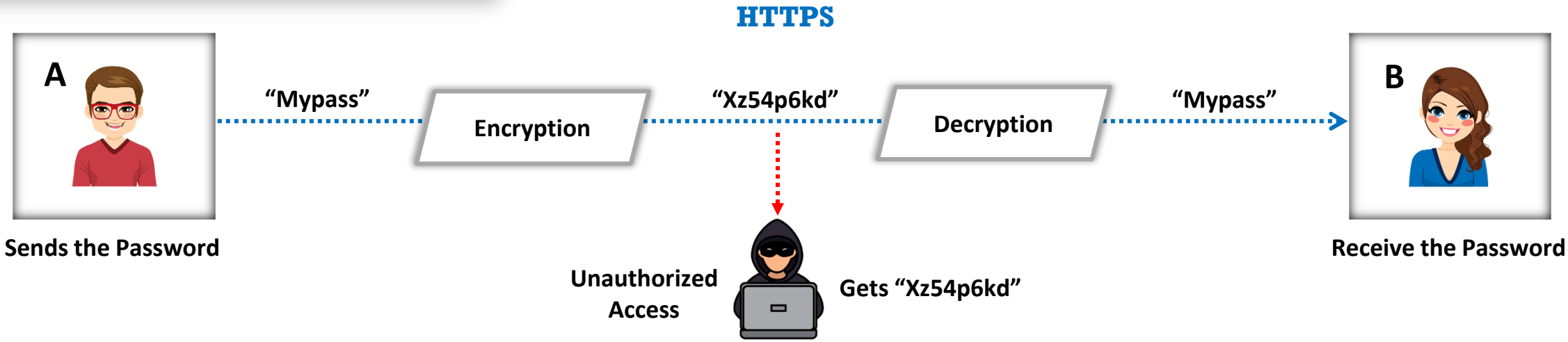


Note: Not all Web browsers and servers support S-HTTP

Hypertext Transfer Protocol Secure (HTTPS)



- Hypertext transfer protocol secure (HTTPS) ensures **secure communication** between two computers over HTTP
- The connection is **encrypted** using a transport layer security (TLS) or SSL protocol
- It is often used in **confidential online transactions**
- It protects against **man-in-the-middle attacks** since the data are transmitted over an encrypted channel



Transport Layer Security (TLS)

- Transport layer security (TLS) ensures a **secure communication** between client-server applications over the internet
- It **prevents** the network communication from being eavesdropped or tampered

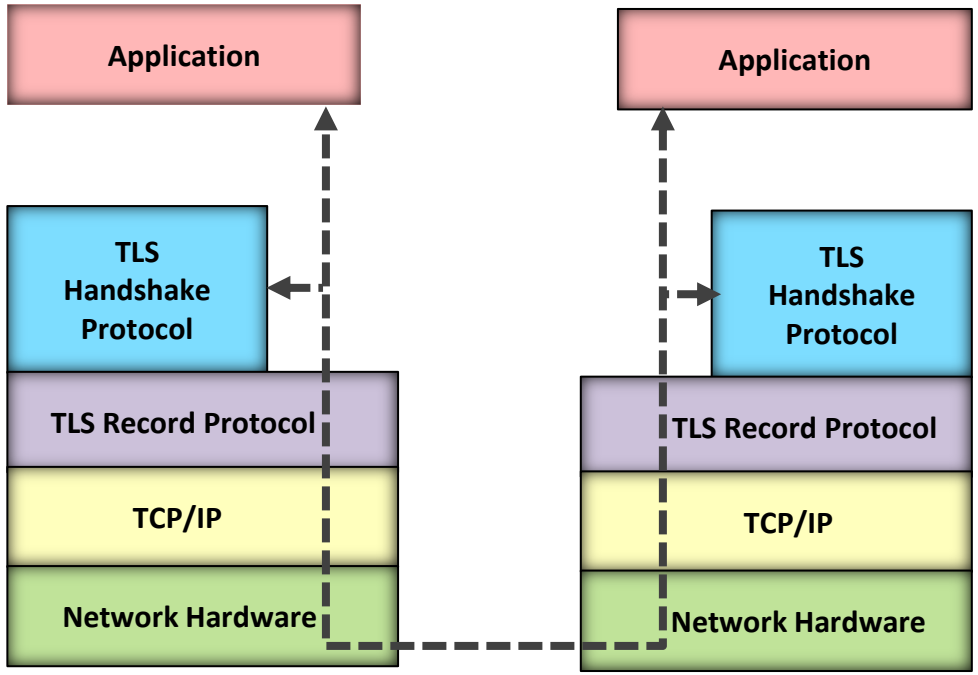
Layers of TLS Protocol

TLS Record Protocol

- It ensures **connection security** with encryption

TLS Handshake Protocol

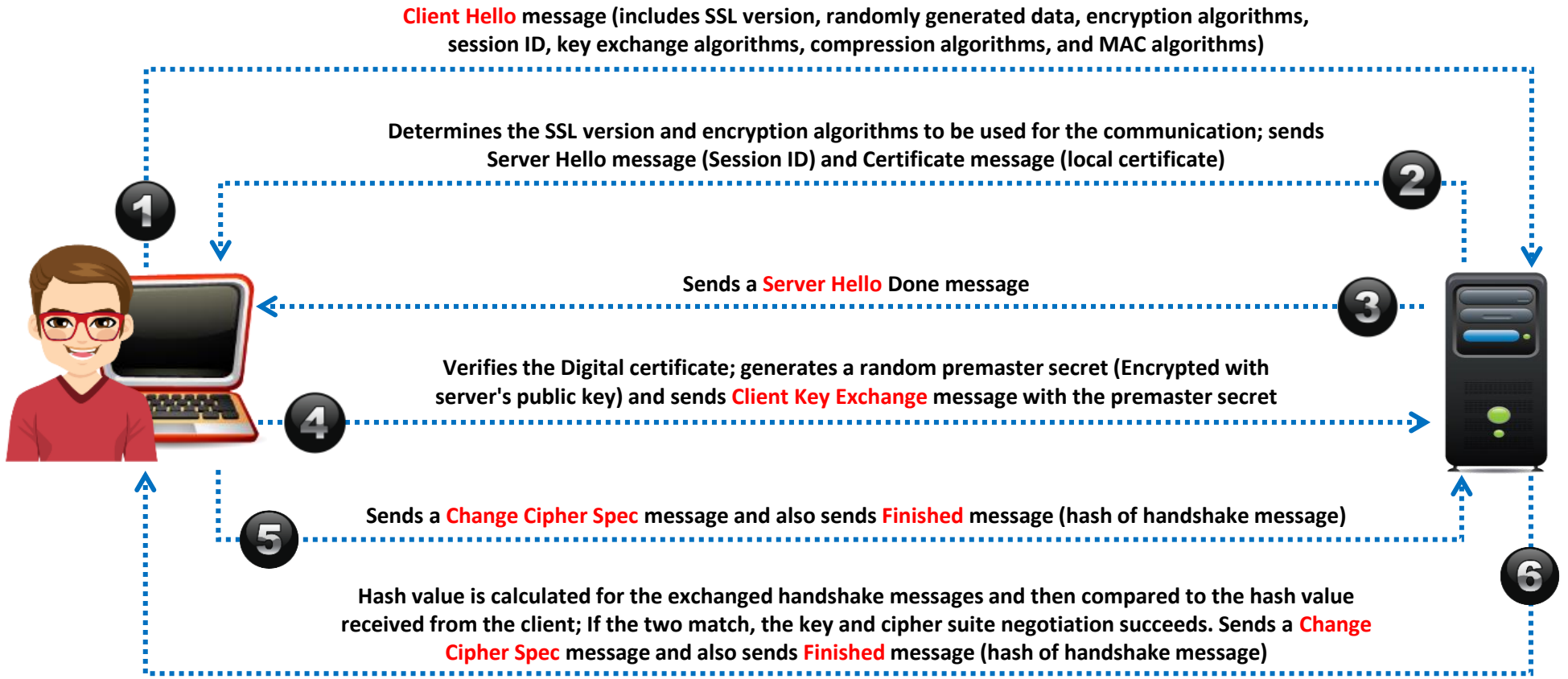
- It ensures server and client **authentication**





Secure Sockets Layer (SSL)

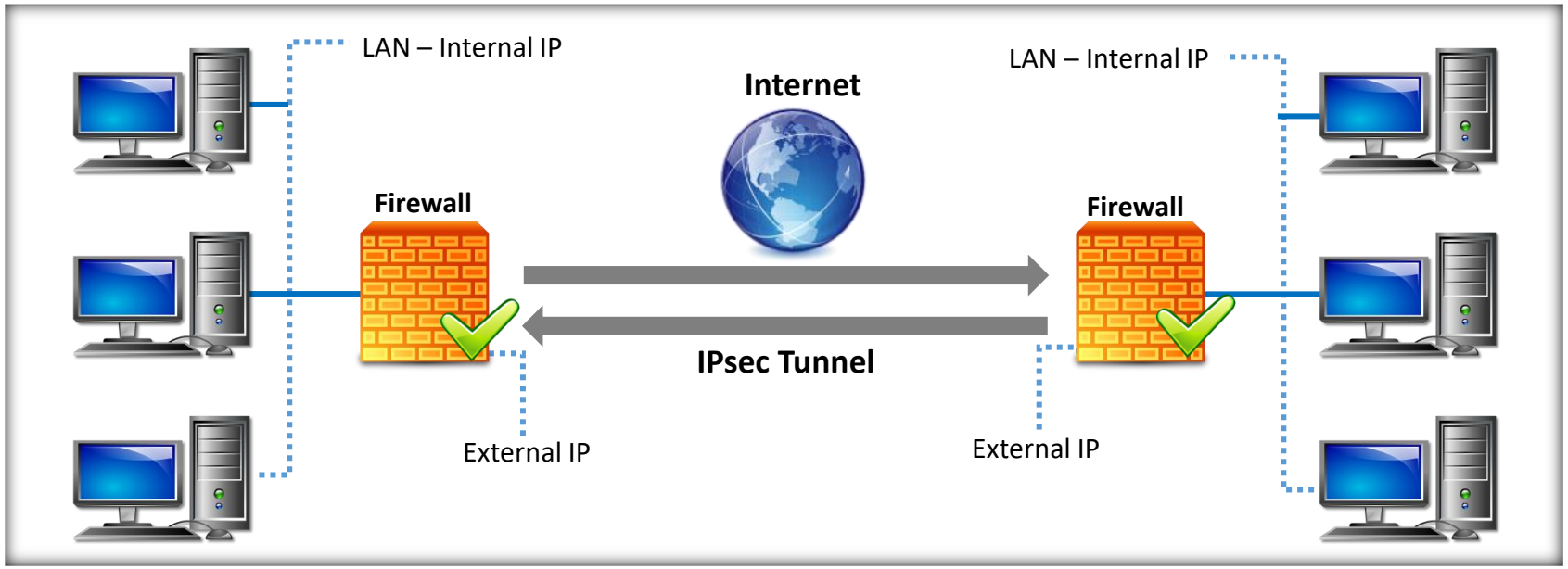
- Secure sockets layer (SSL) was developed by Netscape for **managing the security** of a message transmission on the internet
- It uses the **RSA asymmetric (public key) encryption** to encrypt data transferred over SSL connections



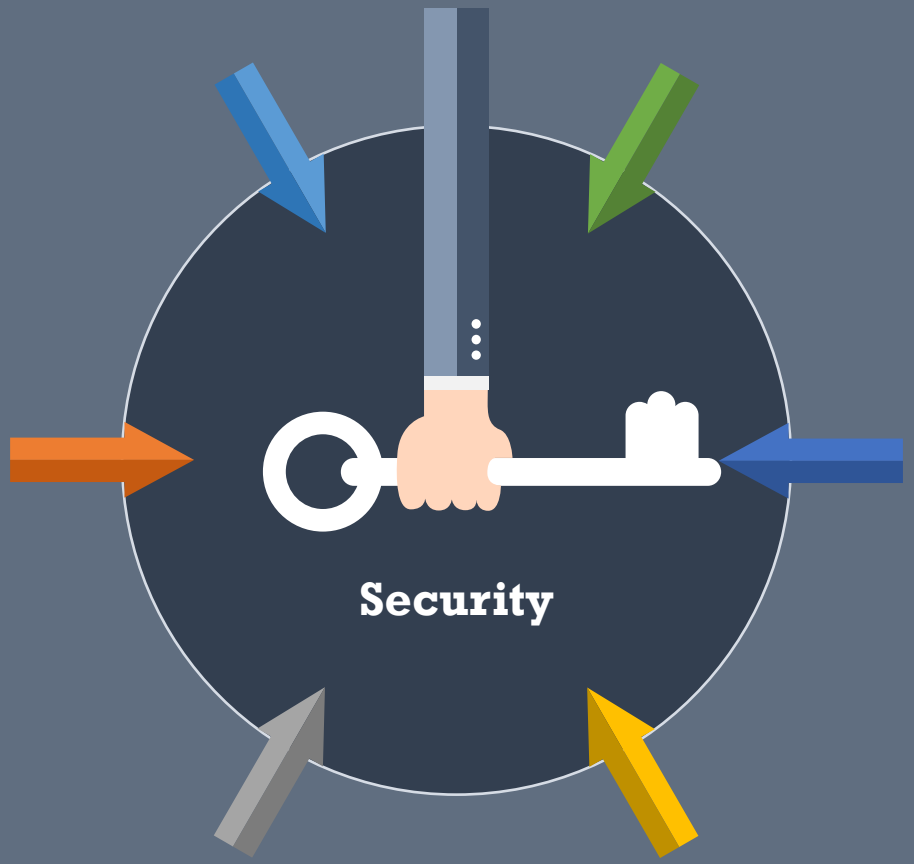
Internet Protocol Security (IPsec)

- Internet protocol security (IPsec) is a network layer protocol that ensures a **secure** IP level communication
- It provides **end-to-end security** at the internet layer of the internet protocol suite

- It **encrypts** and **authenticates** each IP packet in the communication
- It **supports** network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection



Module Summary



This module has discussed the essentials of network security, goal of network defense, and the information assurance (IA) principles

It has discussed benefits and challenges of network defense

It also discussed different types of network defense approaches and types of network security controls

Finally, this module ended with a detailed discussion of various network security protocols

In the next module, we will discuss in detail on identification, authentication, and authorization concepts