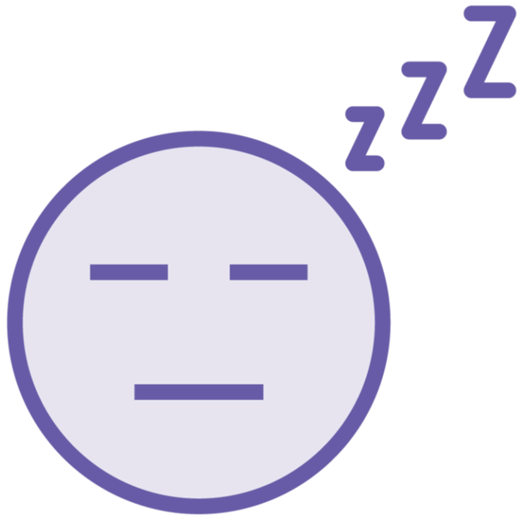
Secure Protocols and Cryptographic Lifecycles

Dr. Lyron H. Andrews
Cryptography for SSCP®

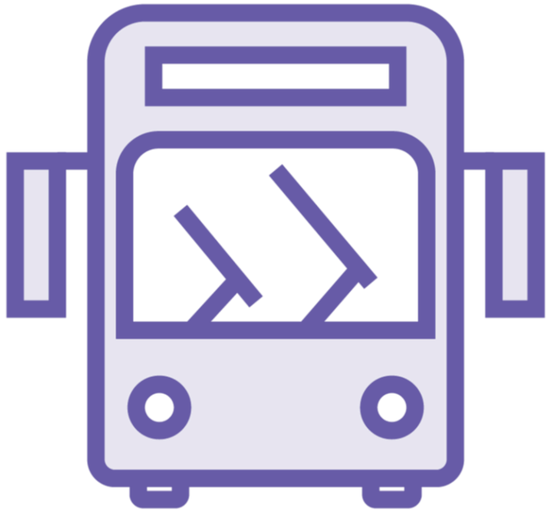
@drlyronandrews | www.profabula.com

Cryptographic Implementation and Use Cases

Three States of Data



Data at rest
Storage systems

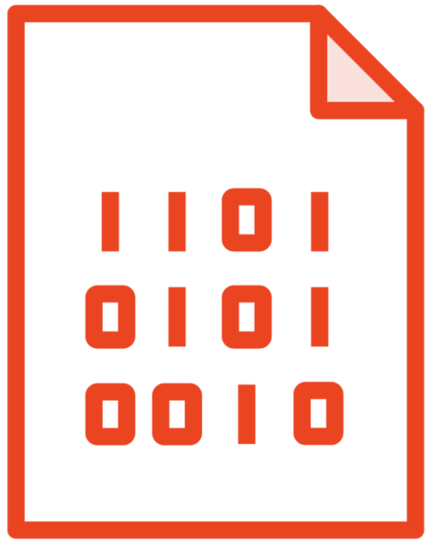


Data in transit
Moving locations

Data in use
Interaction with systems/people

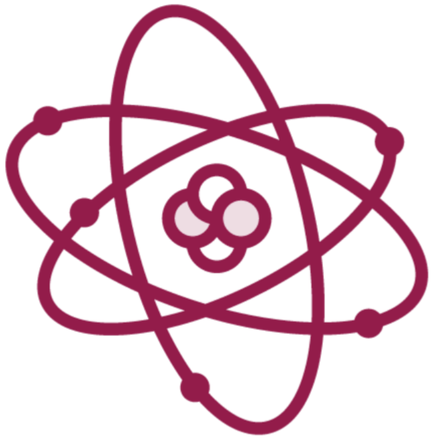
Primary Use Cases

Disk encryption



File encryption

Non-repudiation



Transport encryption

Cryptographic Protocols and Services – Internet Protocol Security (IPSEC)

IPSEC Main Components

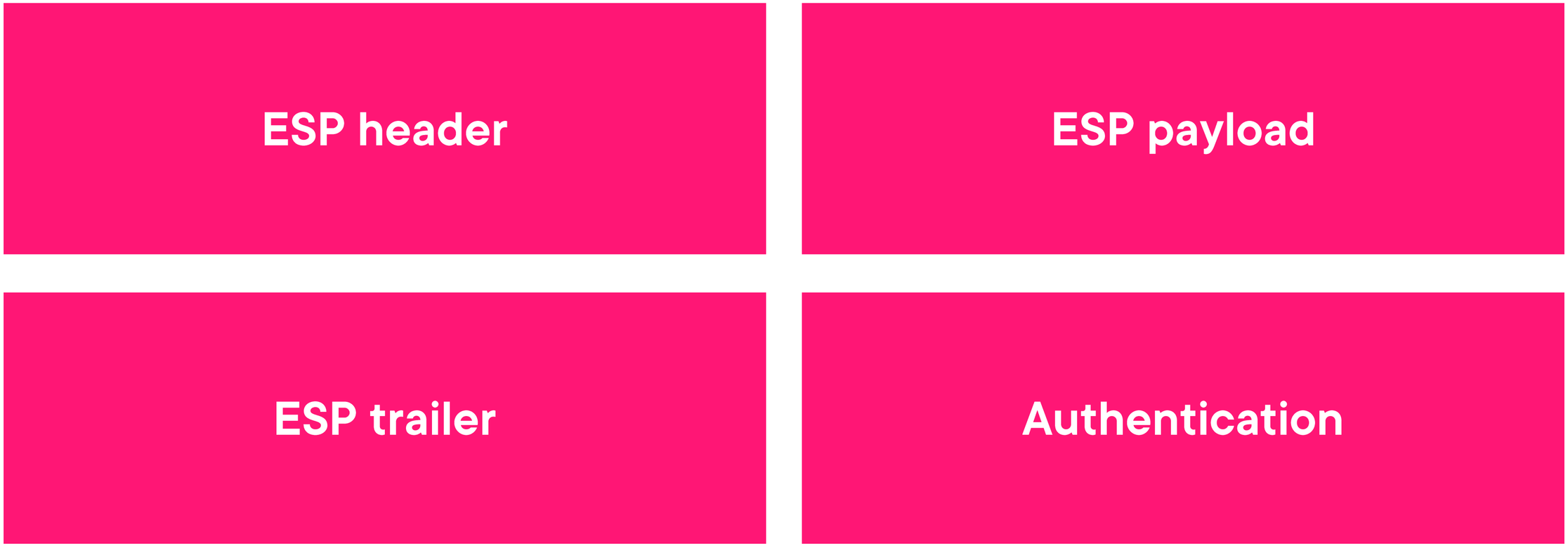
Authentication Header (AH)

Proves identity of source IP

Encapsulating Security Payload (ESP)

Encrypts IP packets and ensures integrity

Encapsulating Security Payload (ESP)



IPSEC Main Components

Authentication Header (AH)

Proves identity of source IP

Encapsulating Security Payload (ESP)

Encrypts IP packets and ensures integrity

Security Association (SA)

Endpoint communications

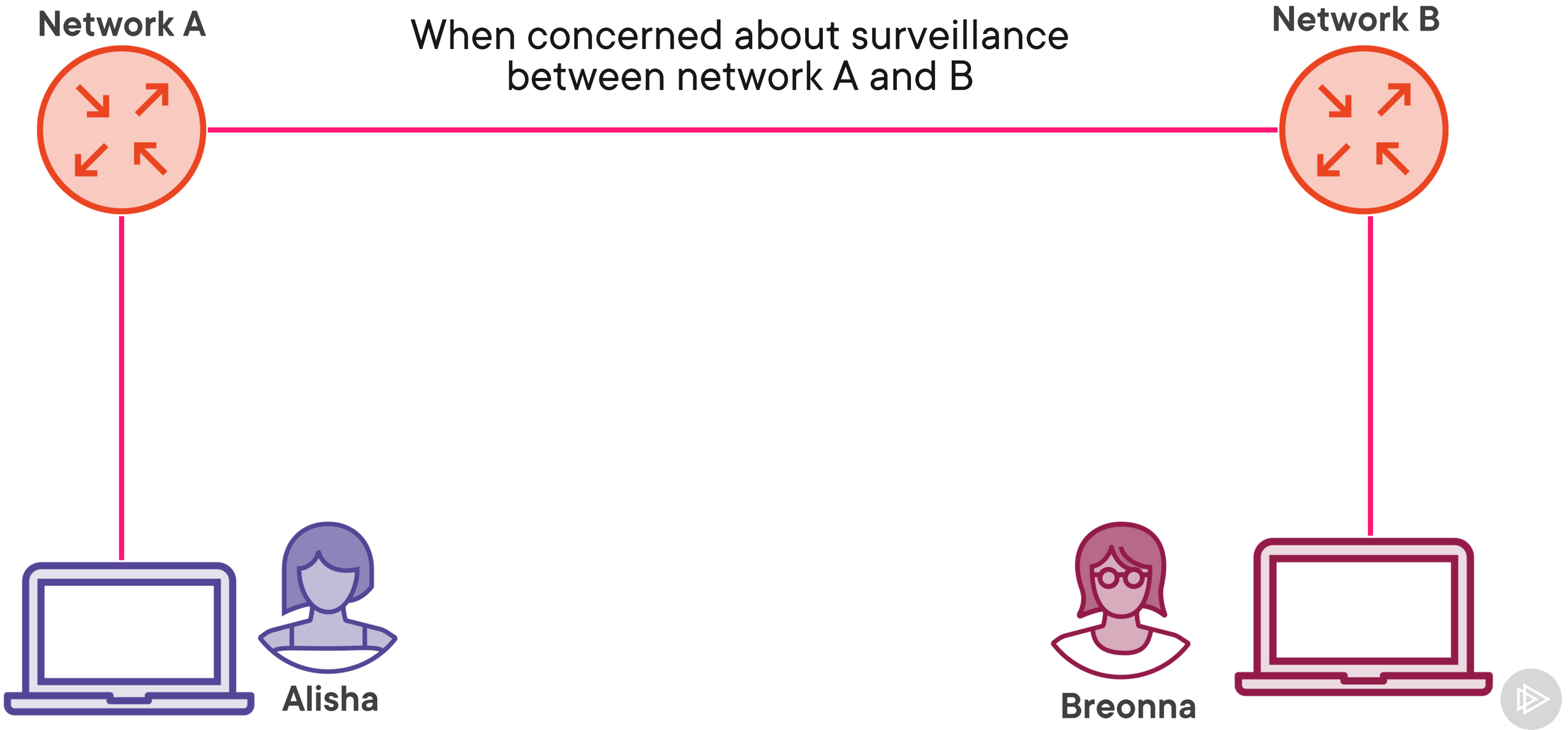
Internet Key Exchange (IKE)

Enables exchange of cryptographic information

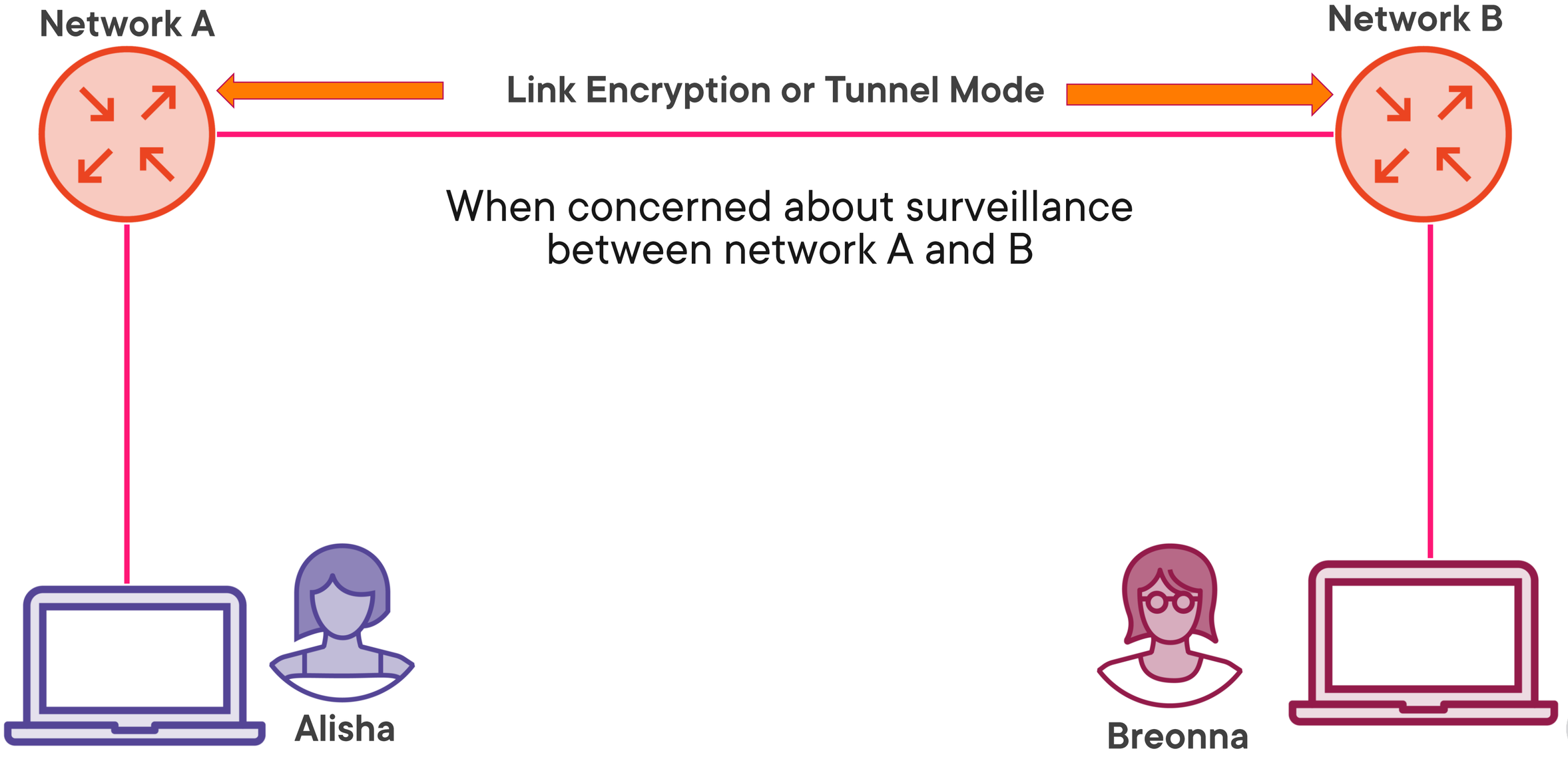
Transport and Tunnel Mode

End-to-end or link encryption

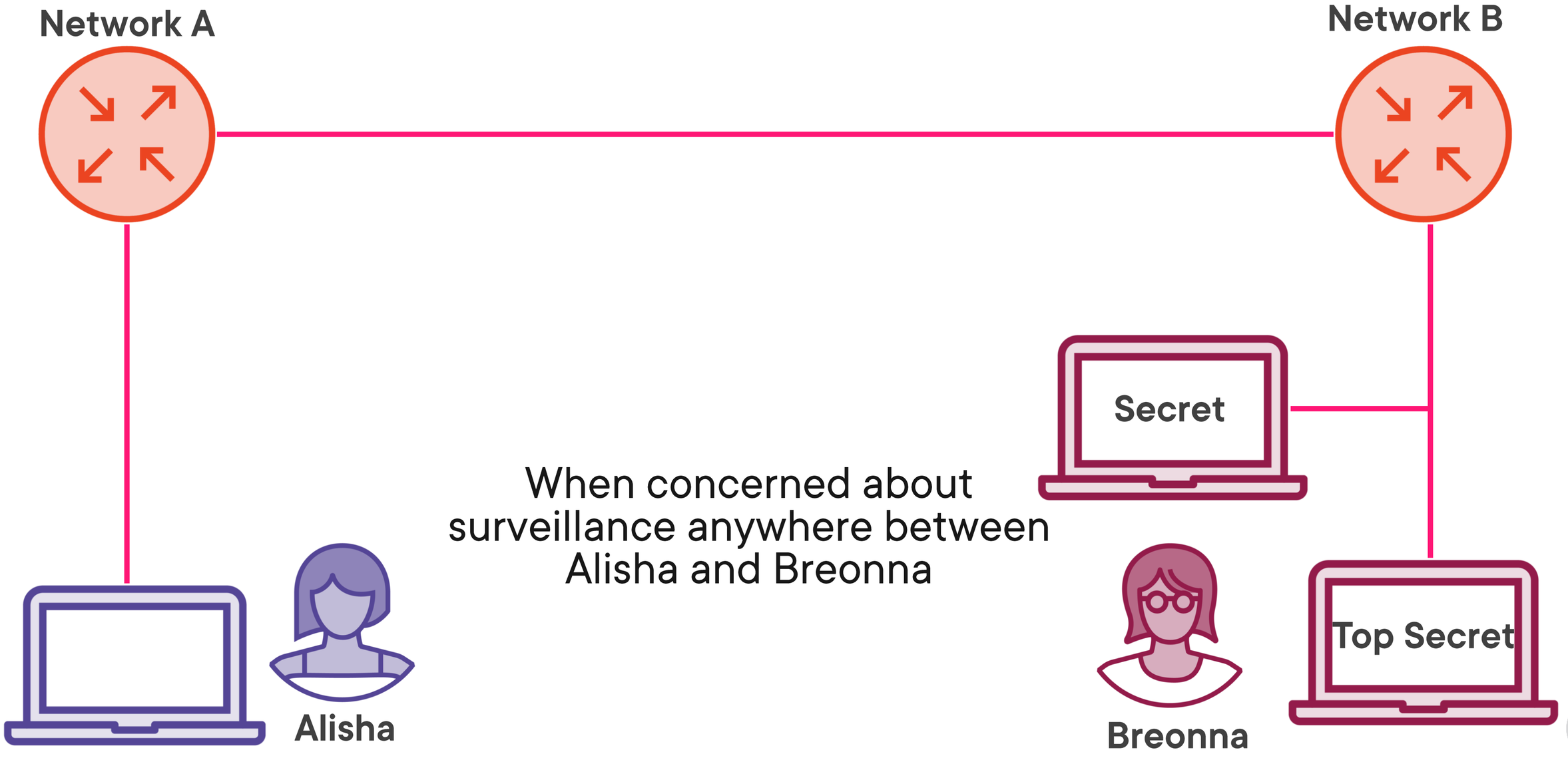
IPSEC Transport and Tunnel Mode



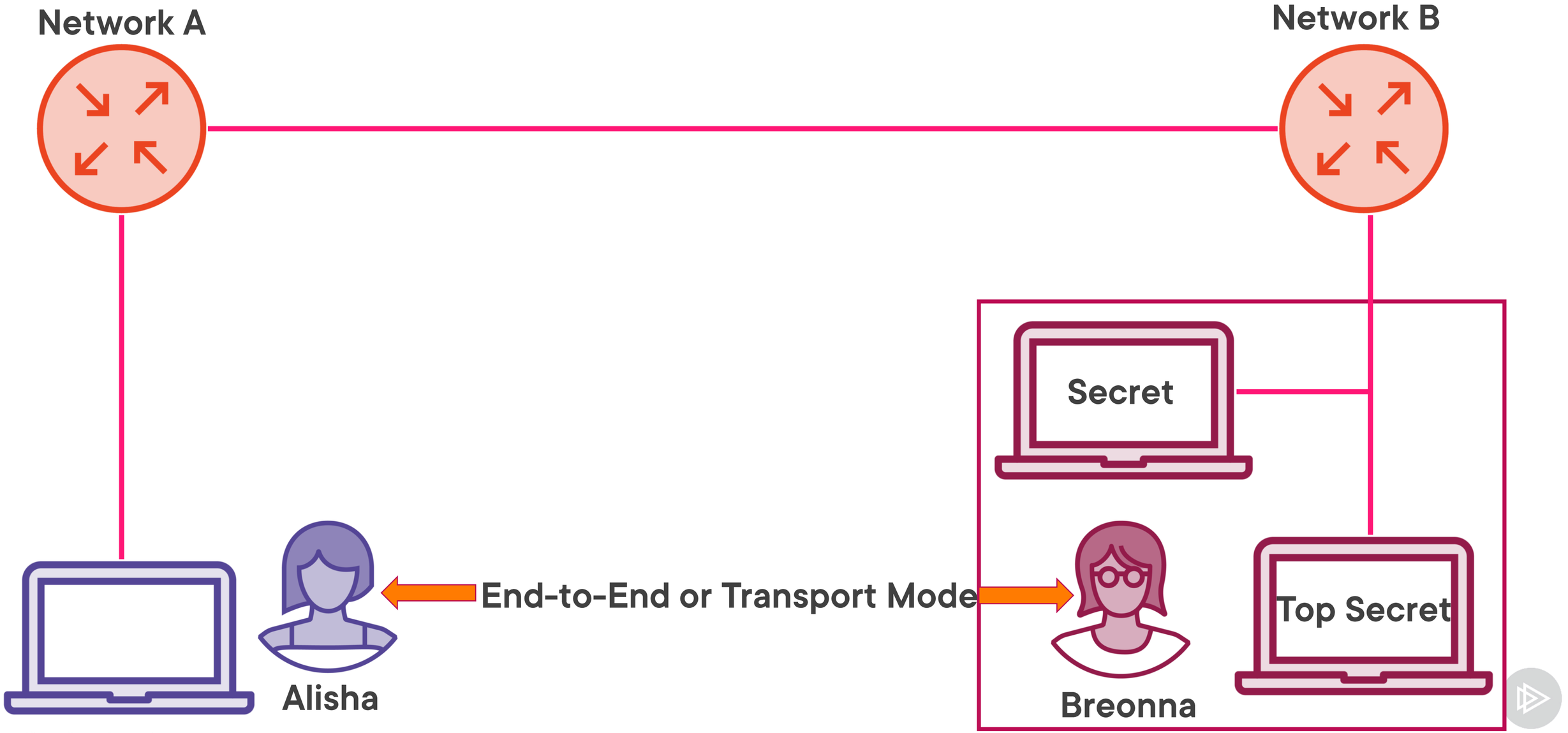
IPSEC Transport and Tunnel Mode



IPSEC Transport and Tunnel Mode



IPSEC Transport and Tunnel Mode



Cryptographic Protocols and Services – Transport Layer Security (TLS)

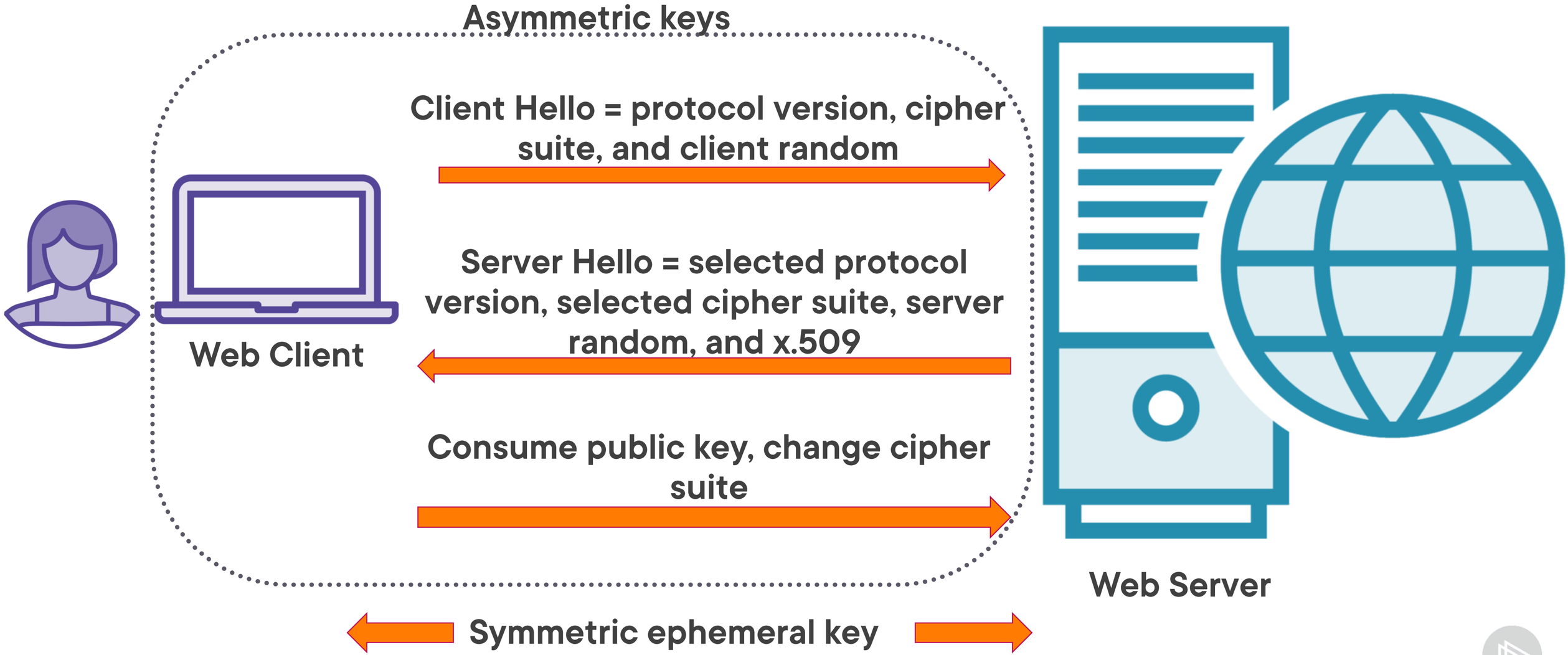
History of SSL/TLS

Started as SSL 2.0

TLS 1.0 and SSL 3.0

TLS 1.1, 1.2, and 1.3

Transport Layer Security (TLS 1.2)



Cryptographic Protocols and Services – Secure/Multipurpose Internet Mail Extensions (S/MIME)

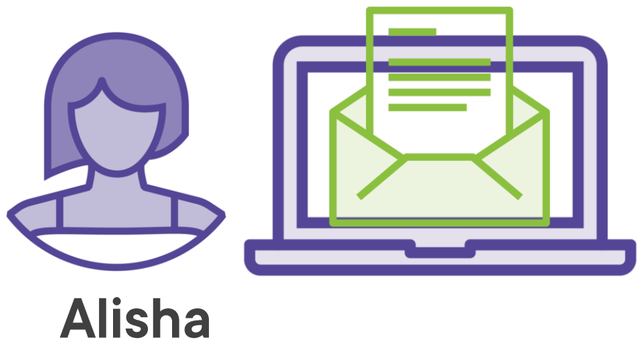
Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

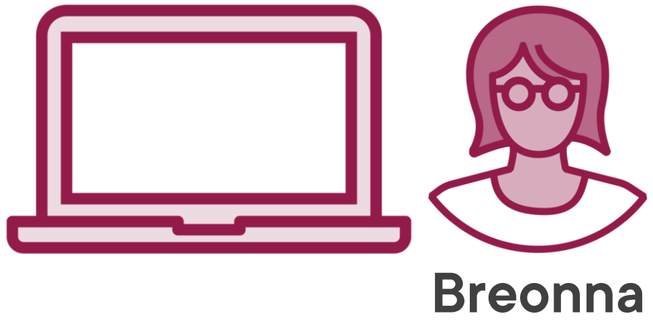
Prevent unauthorized disclosure

Prove sender identity

Maintain message integrity

Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities



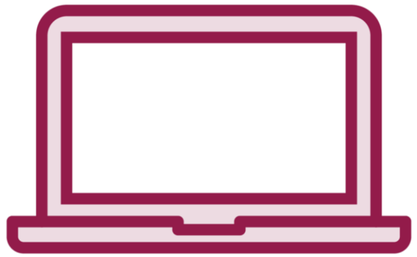


Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Alisha

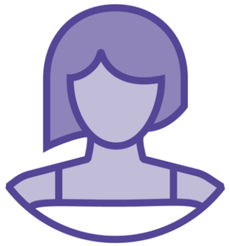
Alisha's private key

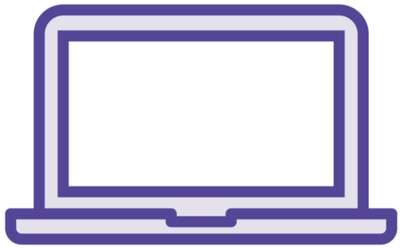
Digitally signs message



Breonna

Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities



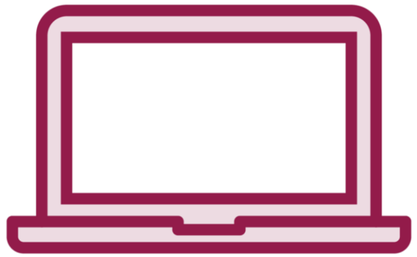


Alisha

Breonna's public key

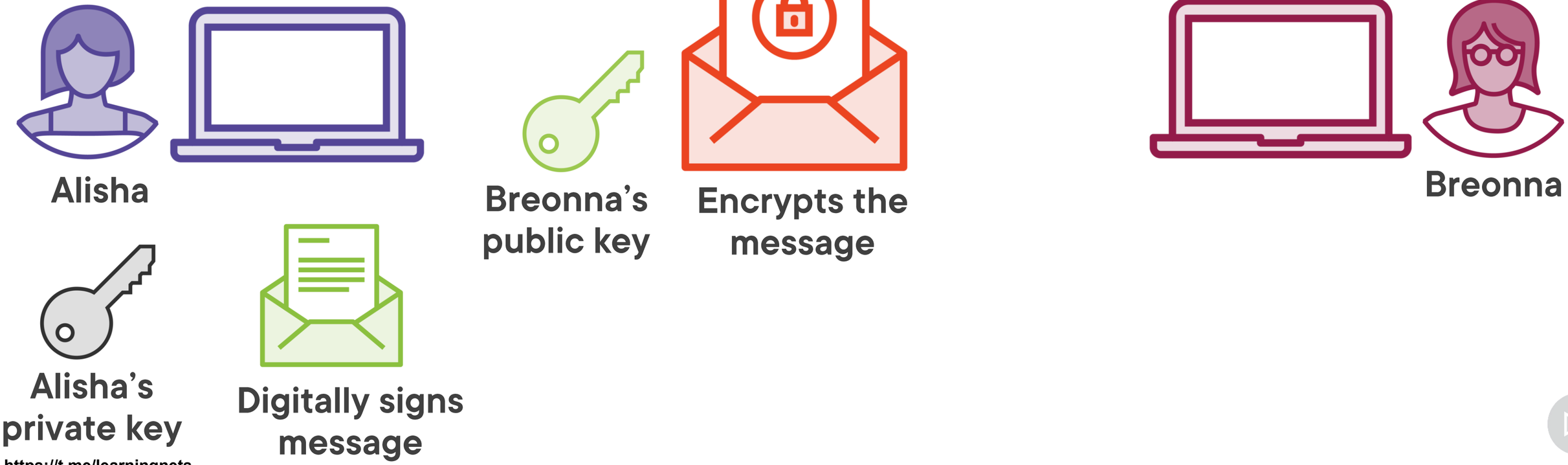
Alisha's private key

Digitally signs message



Breonna

Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

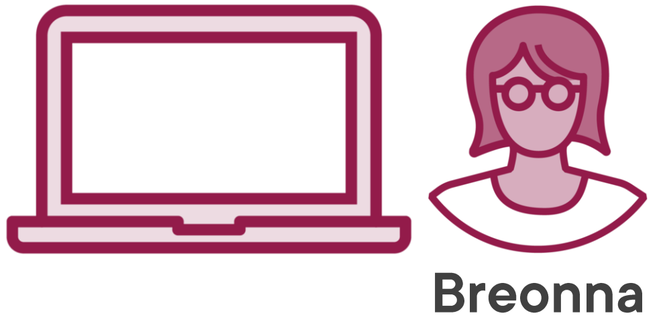


Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Alisha

Breonna's private key

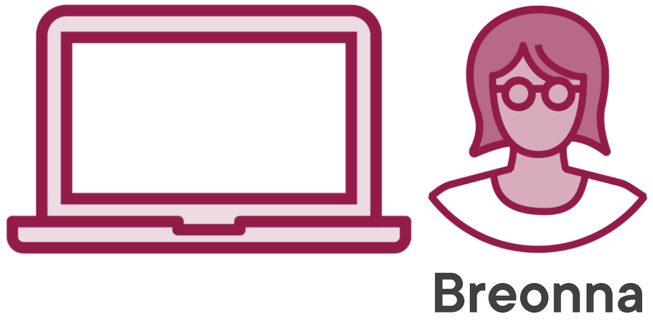
Decrypts the message



Breonna

Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Alisha



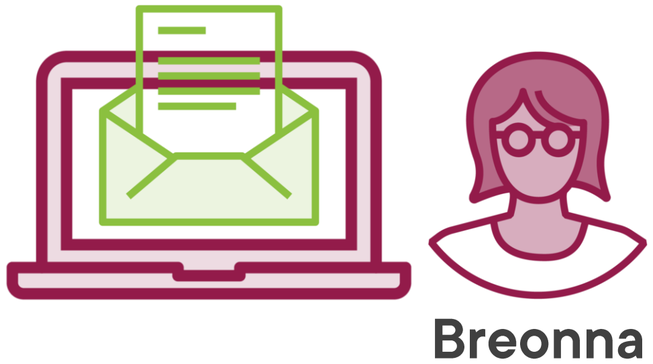
Breonna

Alisha's public key

Verifies sender

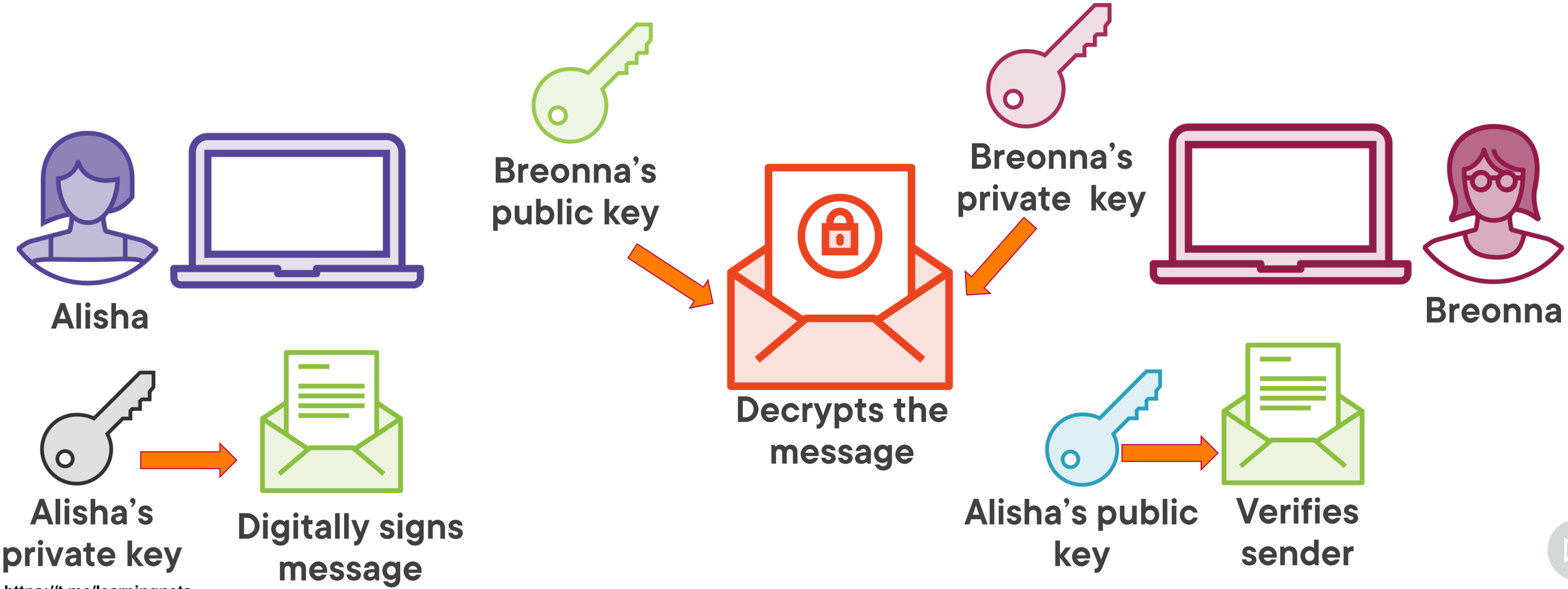
Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities

Alisha



Breonna

Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities



Cryptographic Protocols and Services – DMARC, SPF, and DKIM

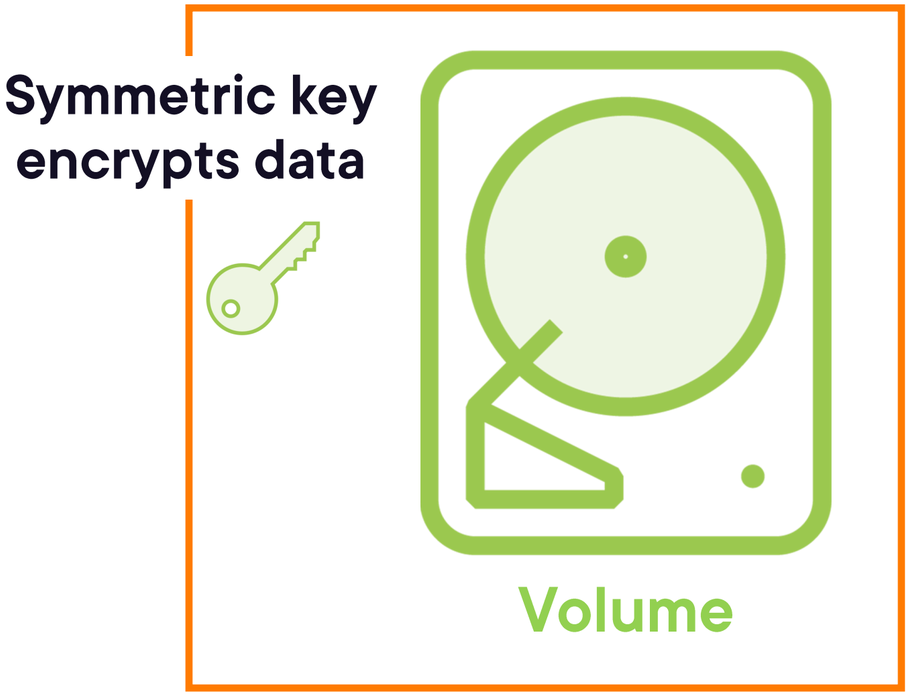
DomainKeys Identified Mail (DKIM) permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message.

Sender Policy Framework (SPF) specifies which hosts are permitted to use and organization's DNS names, and identity during a mail transaction by compliant mail receivers using the published SPF records to test the authorization.

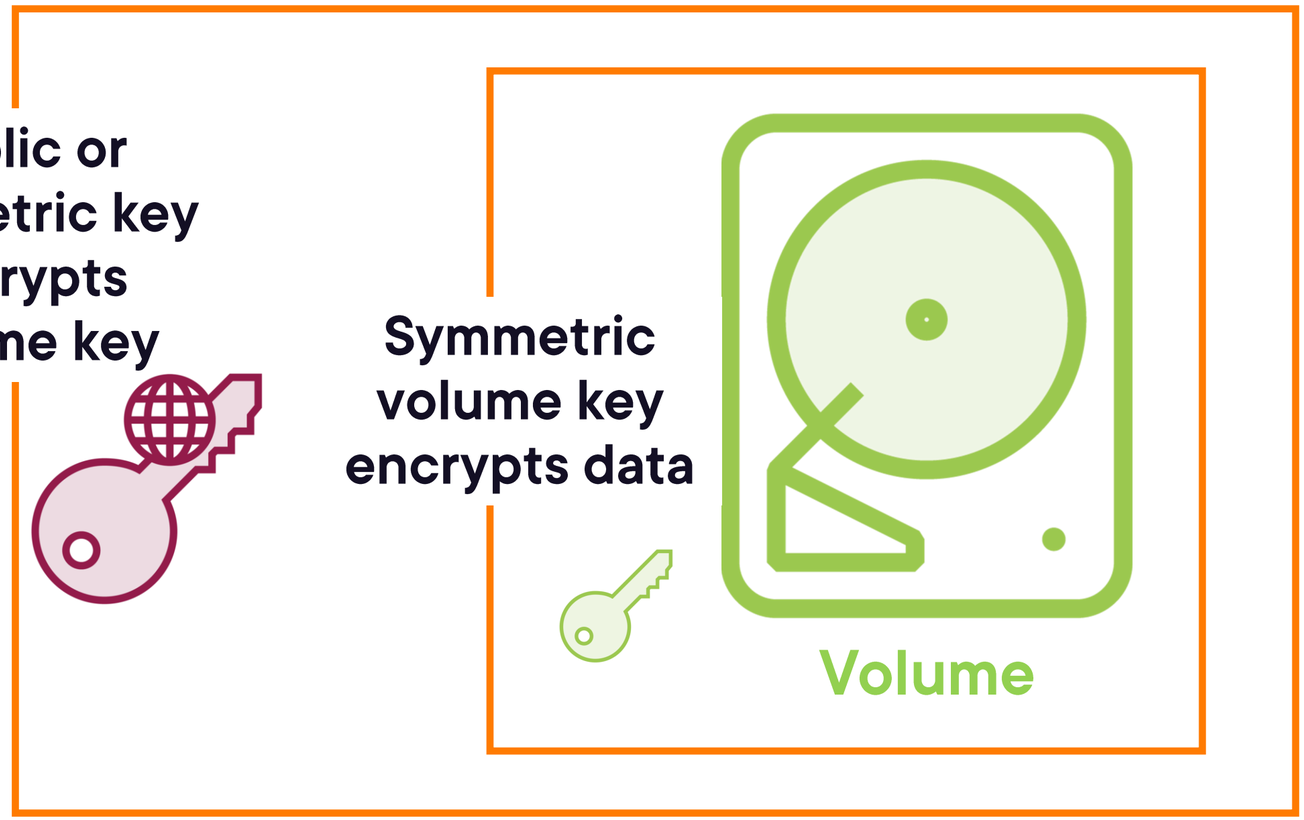
Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a scalable mechanism by which a mail-originatin organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling.

Disk and File Encryption Use Cases

Full Disk Encryption



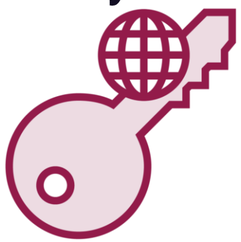
Full Disk Encryption



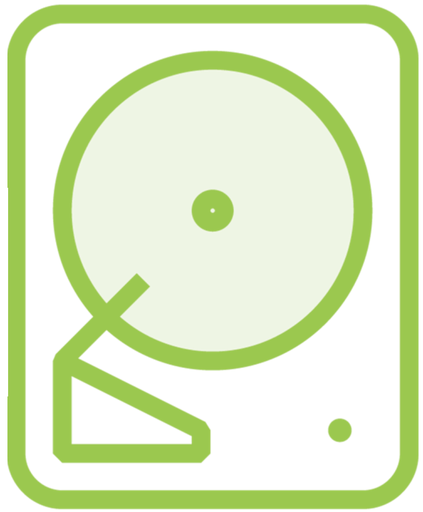
Full Disk Encryption

TPM or user private key decrypts public

Public or symmetric key encrypts volume key

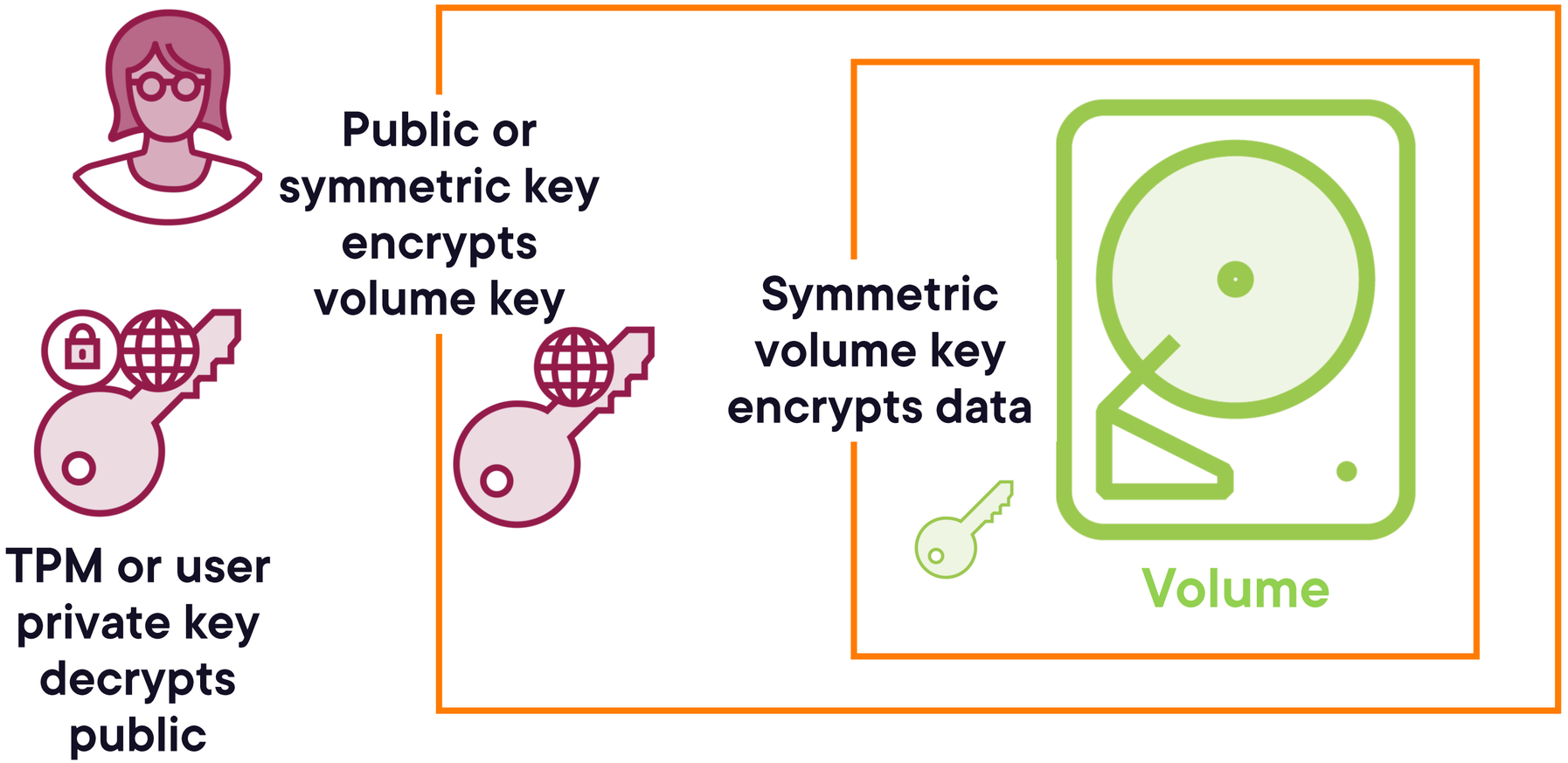


Symmetric volume key encrypts data

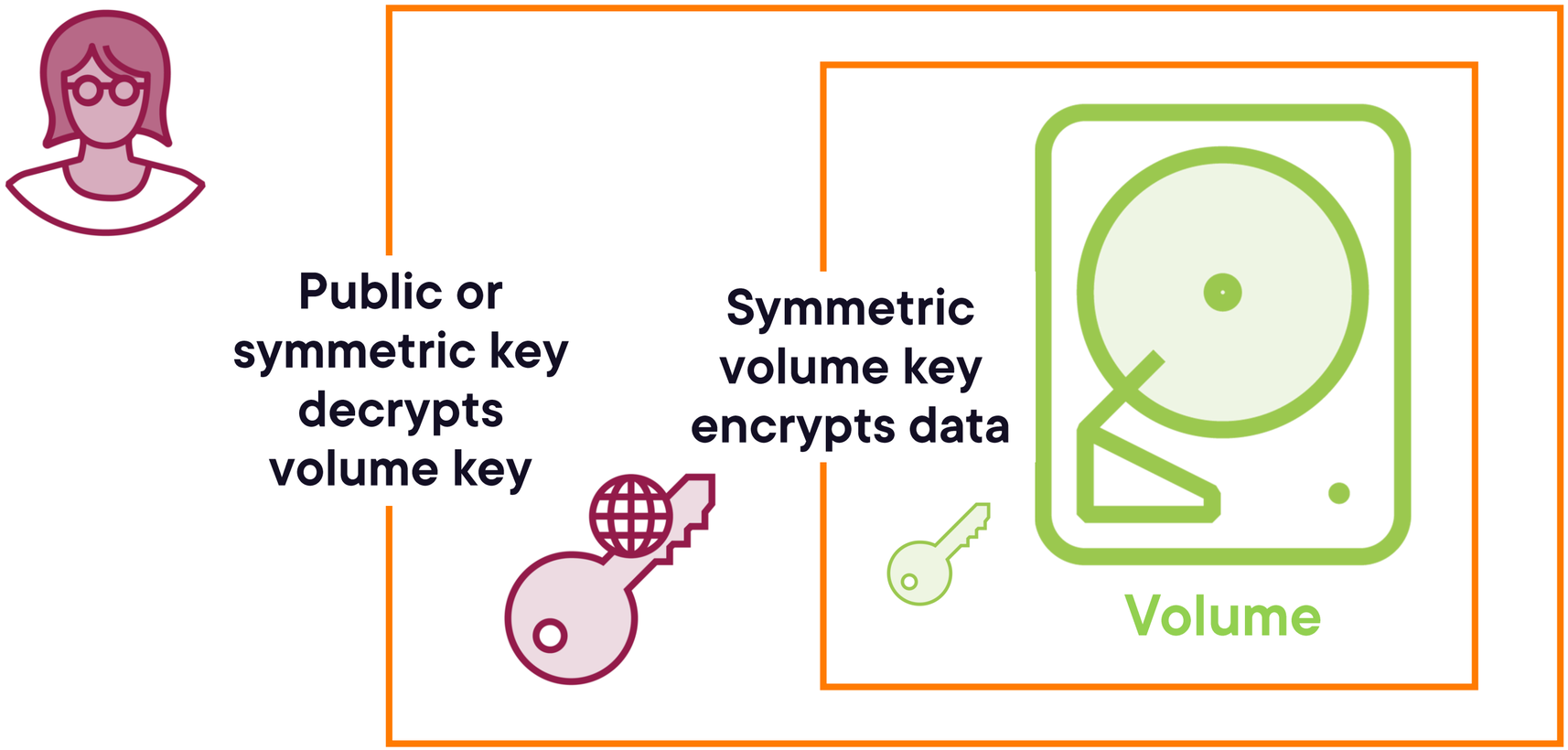


Volume

Full Disk Encryption

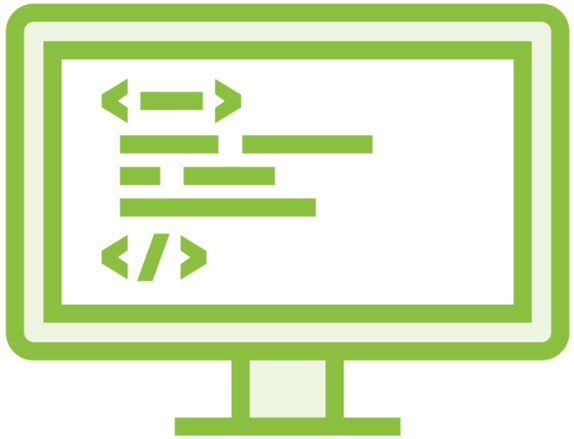


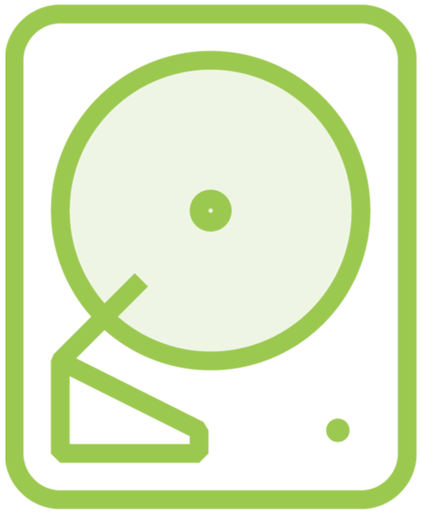
Full Disk Encryption



Full Disk Encryption

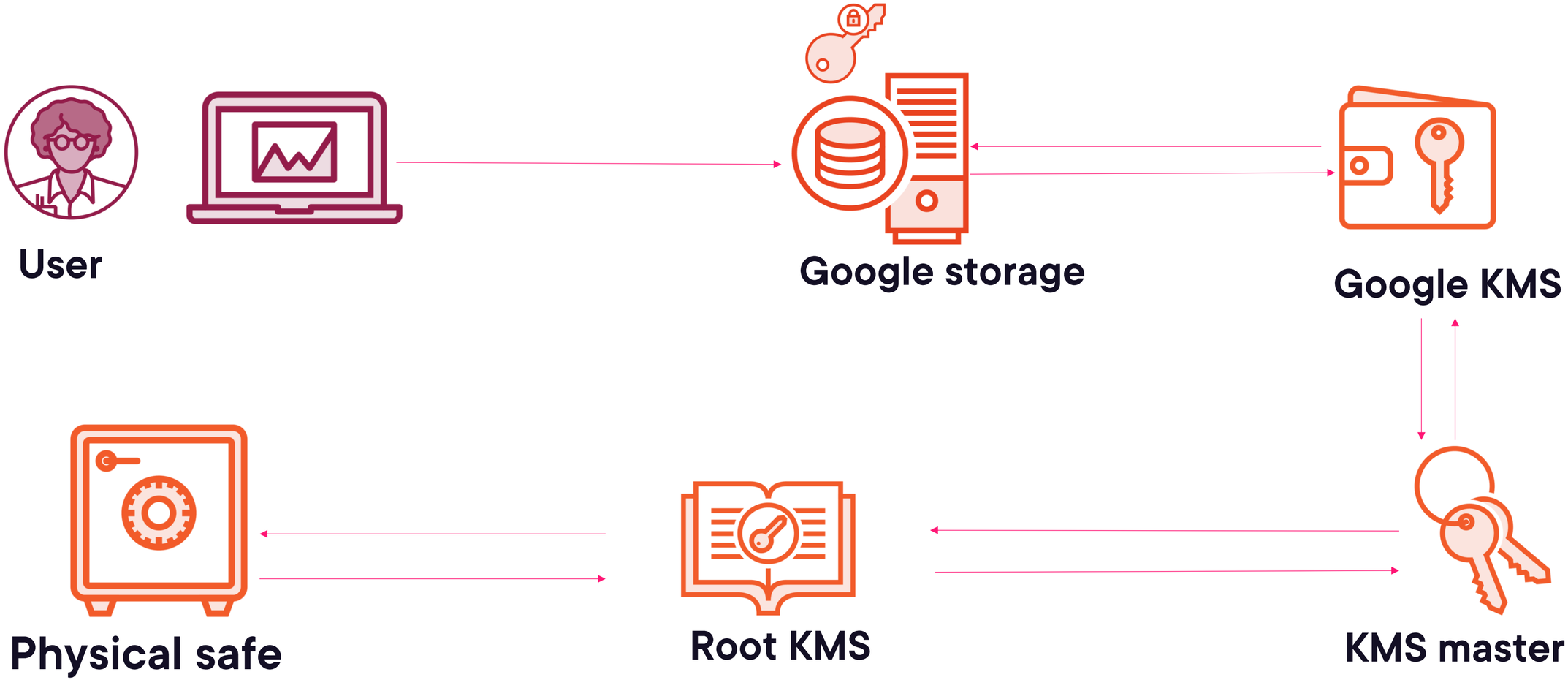
User access to resource granted





Volume

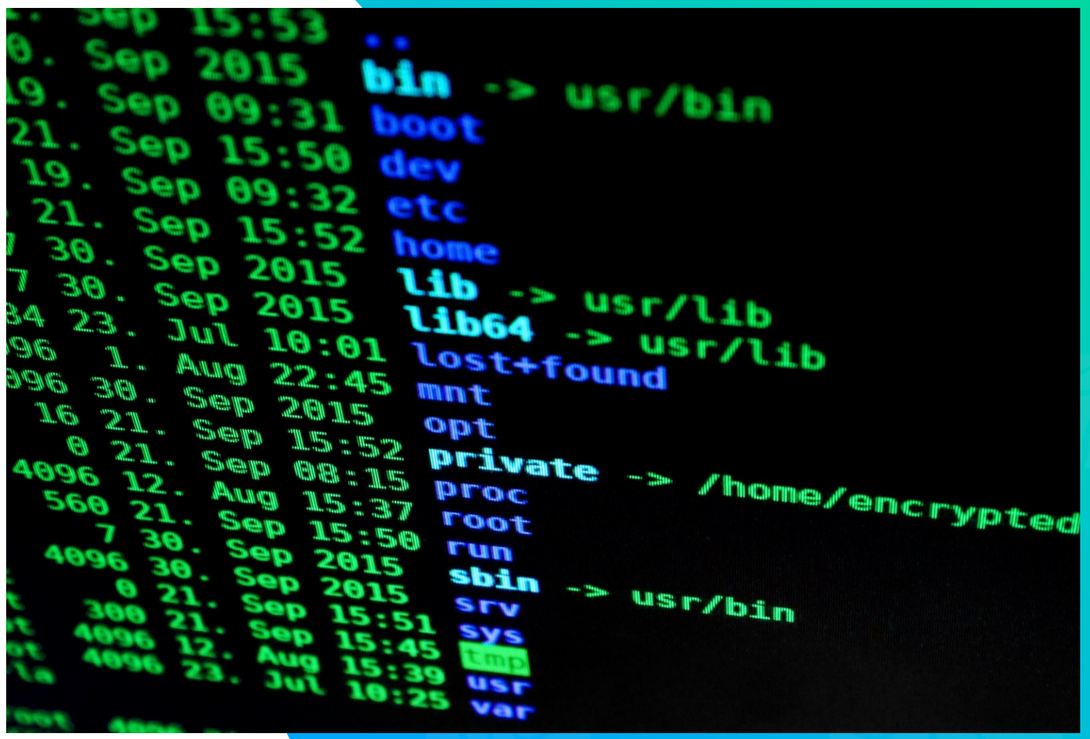
Google Key Wrapping



Public Key Infrastructure Principles

Pretty Good Privacy

Three things that you need to know



1. Public-private key pair algorithm developed in 1991 by Phil Zimmerman
2. Supports message authentication and integrity checking with RSA or DSA
3. Web of Trust

GNU Privacy Guard is an updated PGP use case

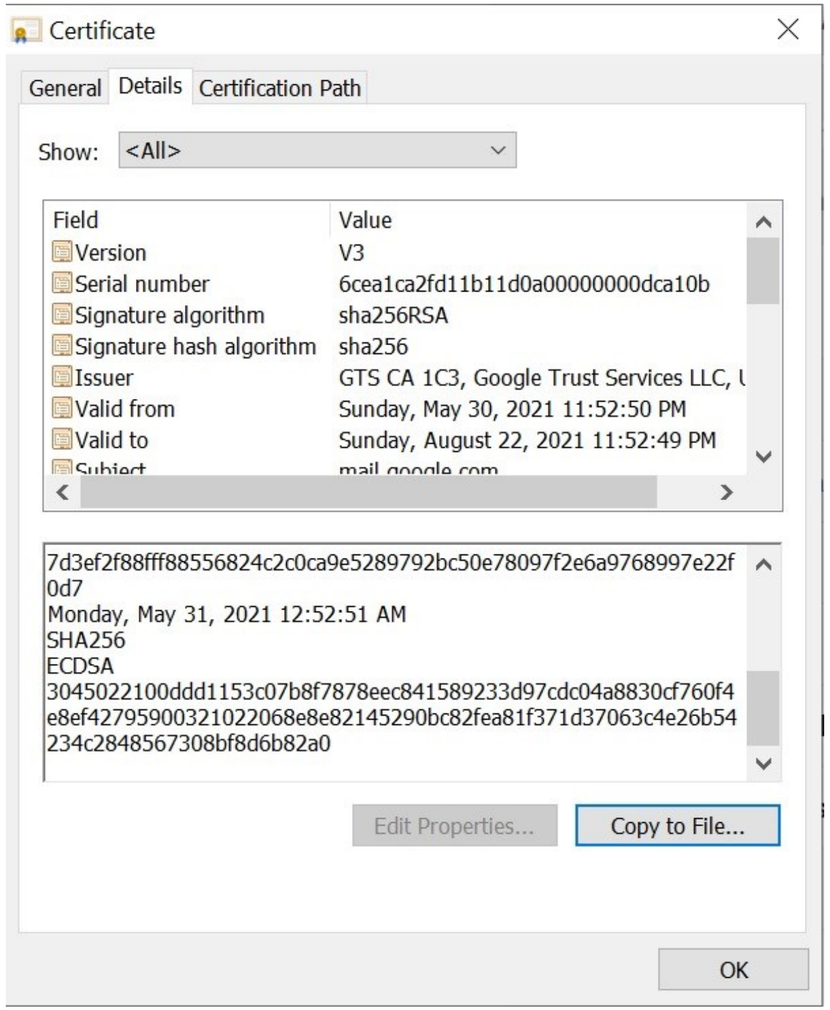
Main Functions of PKI Management

Hierarchical certificate issuance and management

Attestation of entities, trust, and assurance

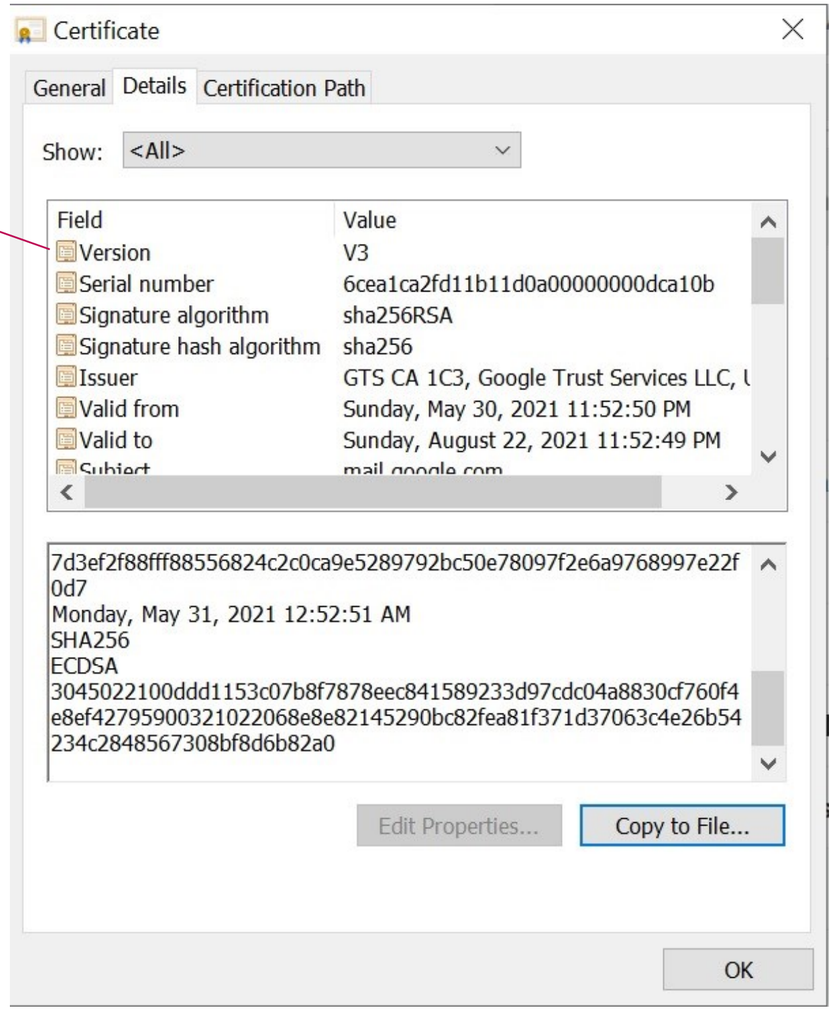
Confidentiality of communication channels

X.509 Components



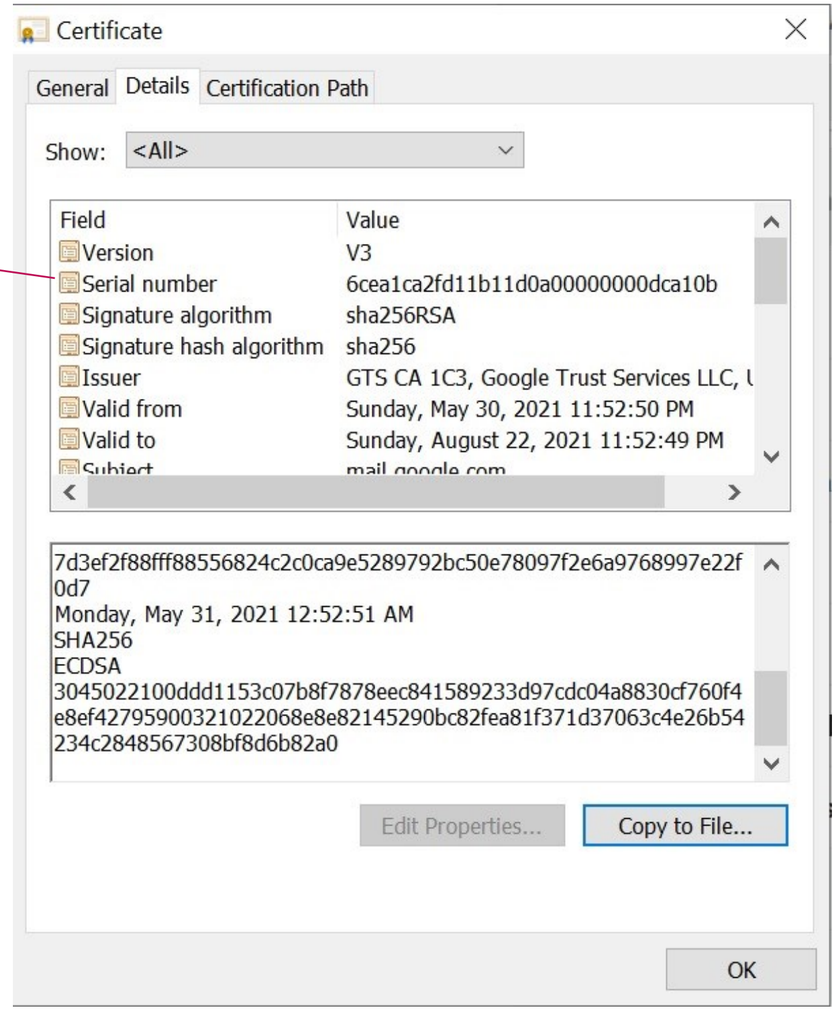
X.509 Components

Version of certificate



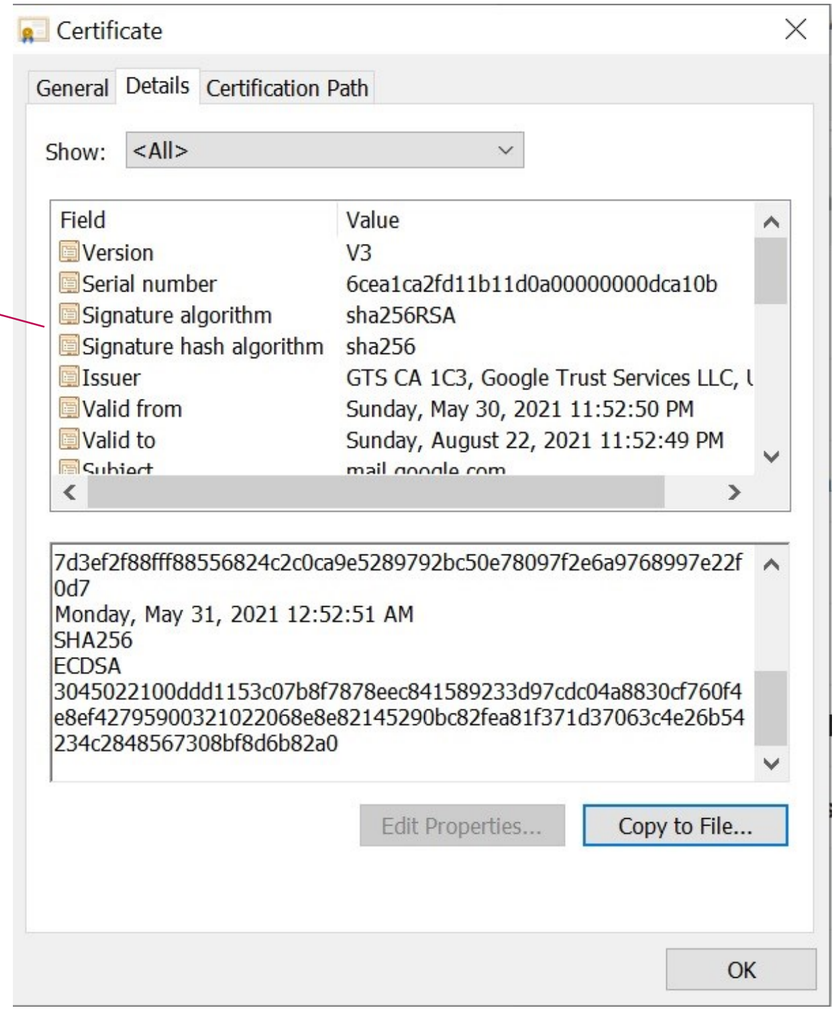
X.509 Components

Positive unique integer



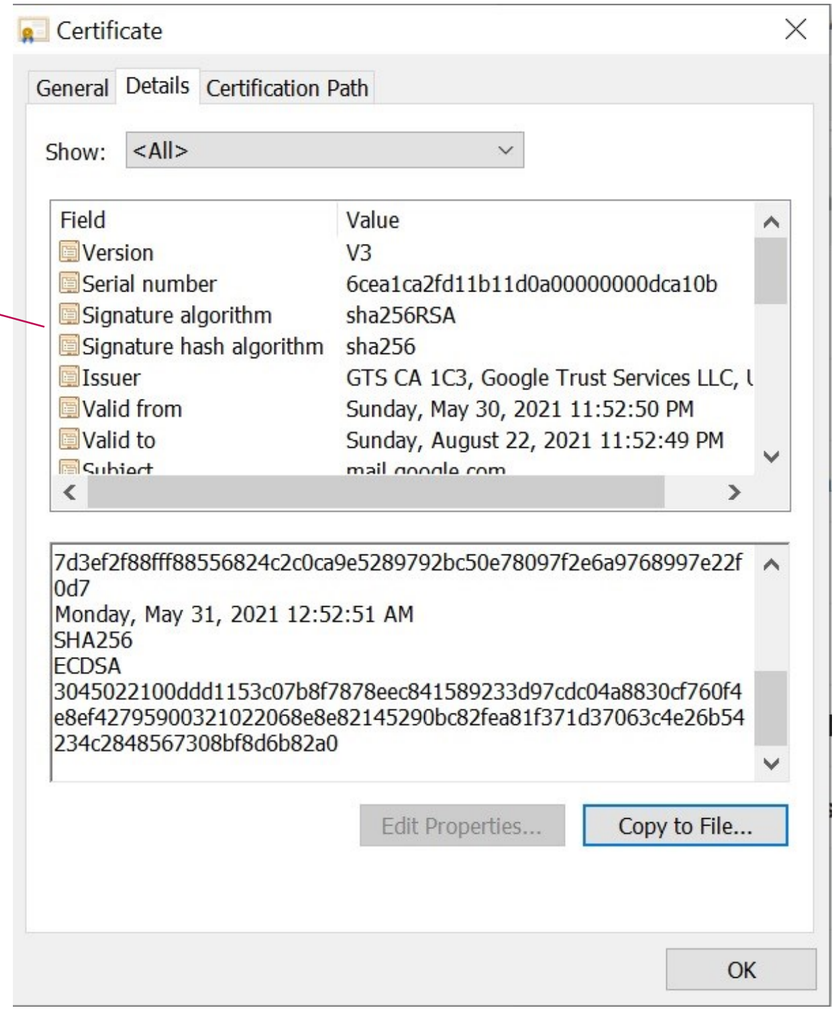
X.509 Components

Algorithm used by CA to sign certificate



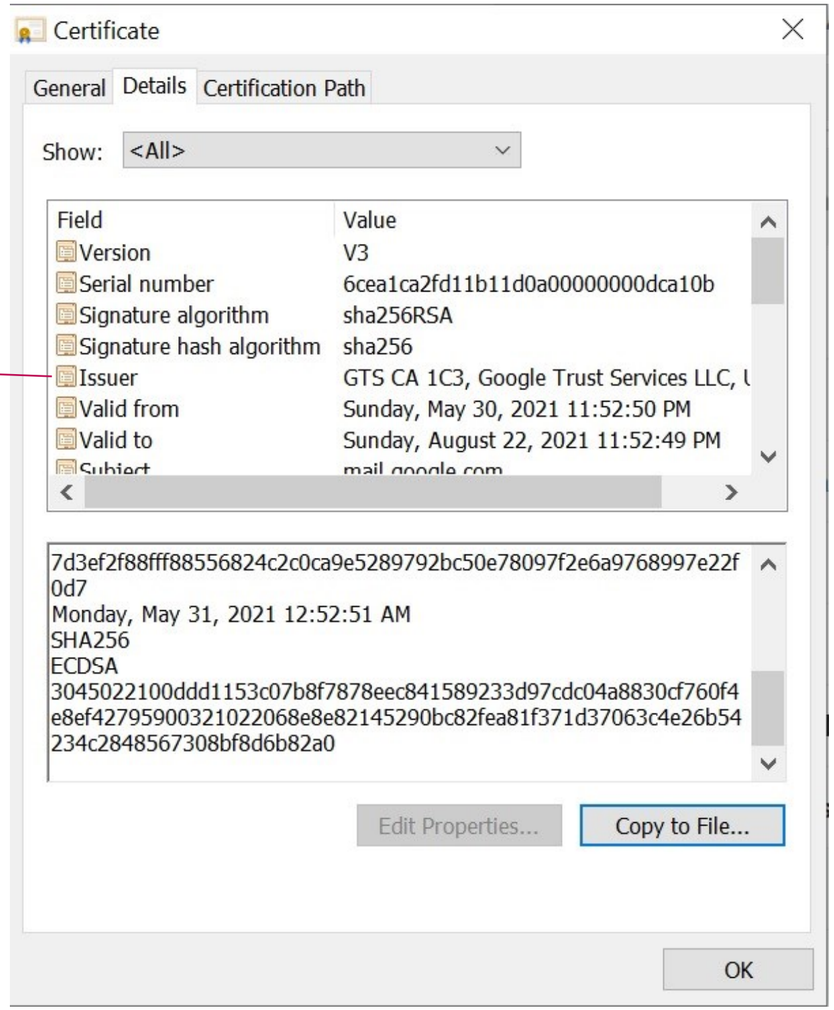
X.509 Components

Algorithm used by CA to sign certificate



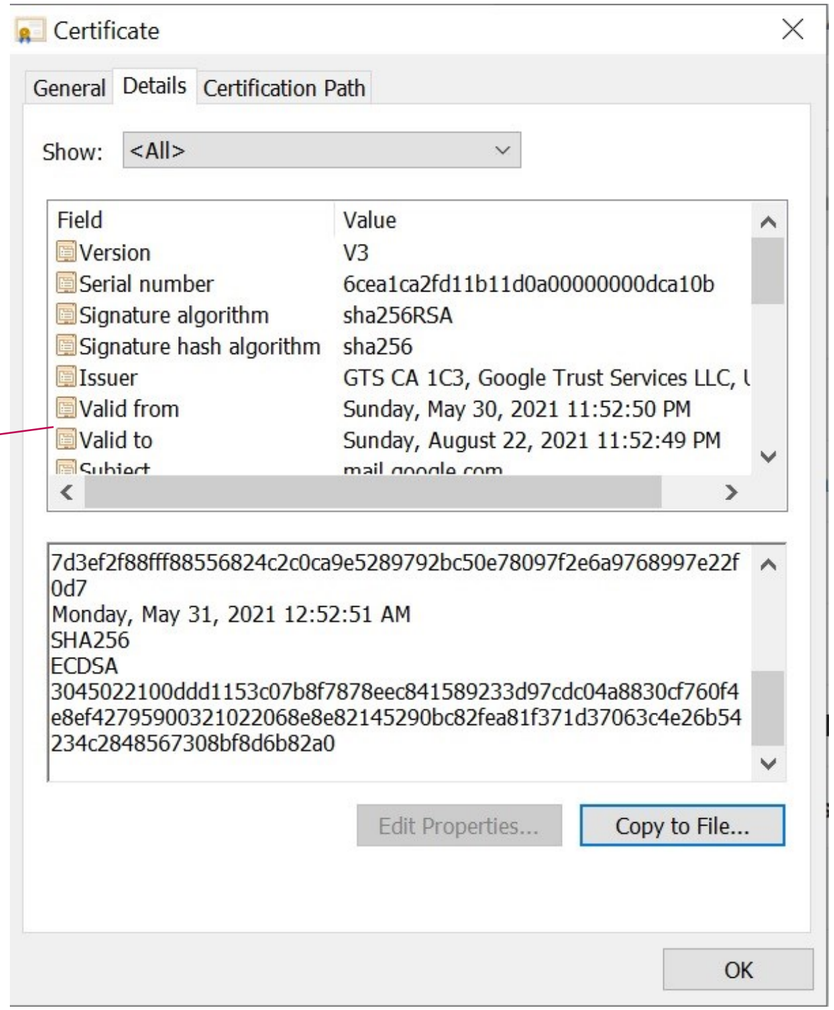
X.509 Components

CA that issues certificate



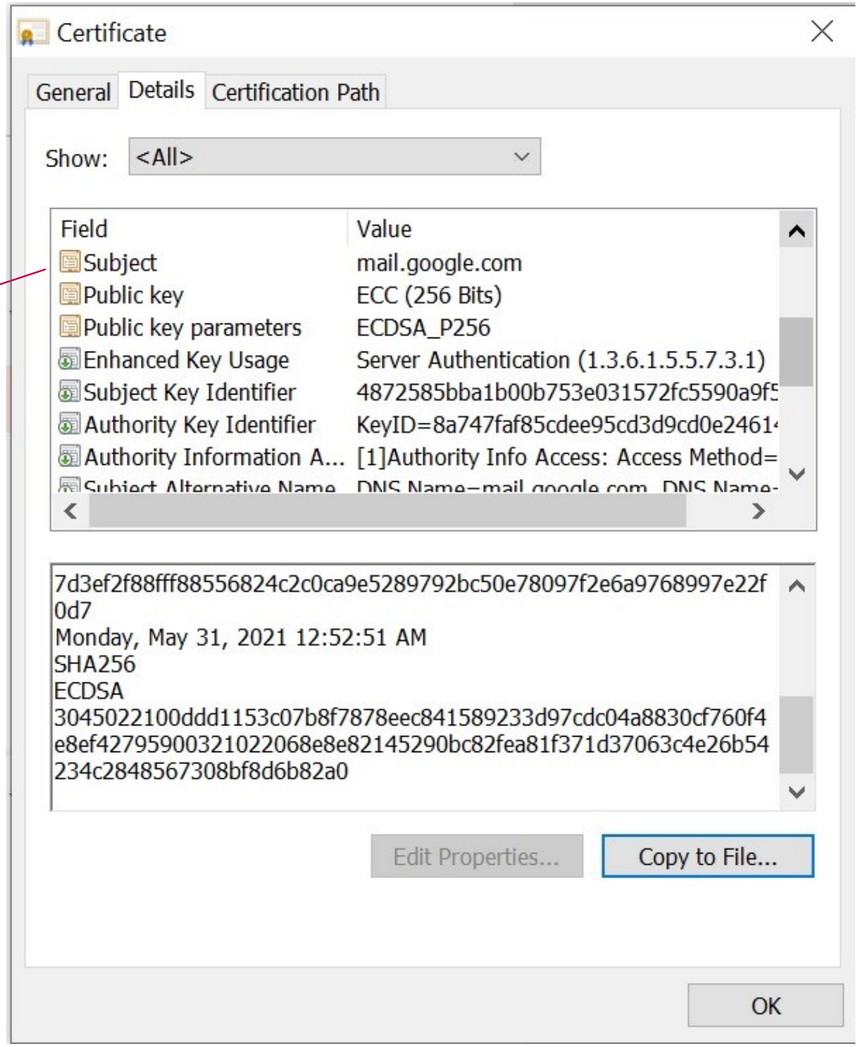
X.509 Components

Length of time certificate is valid



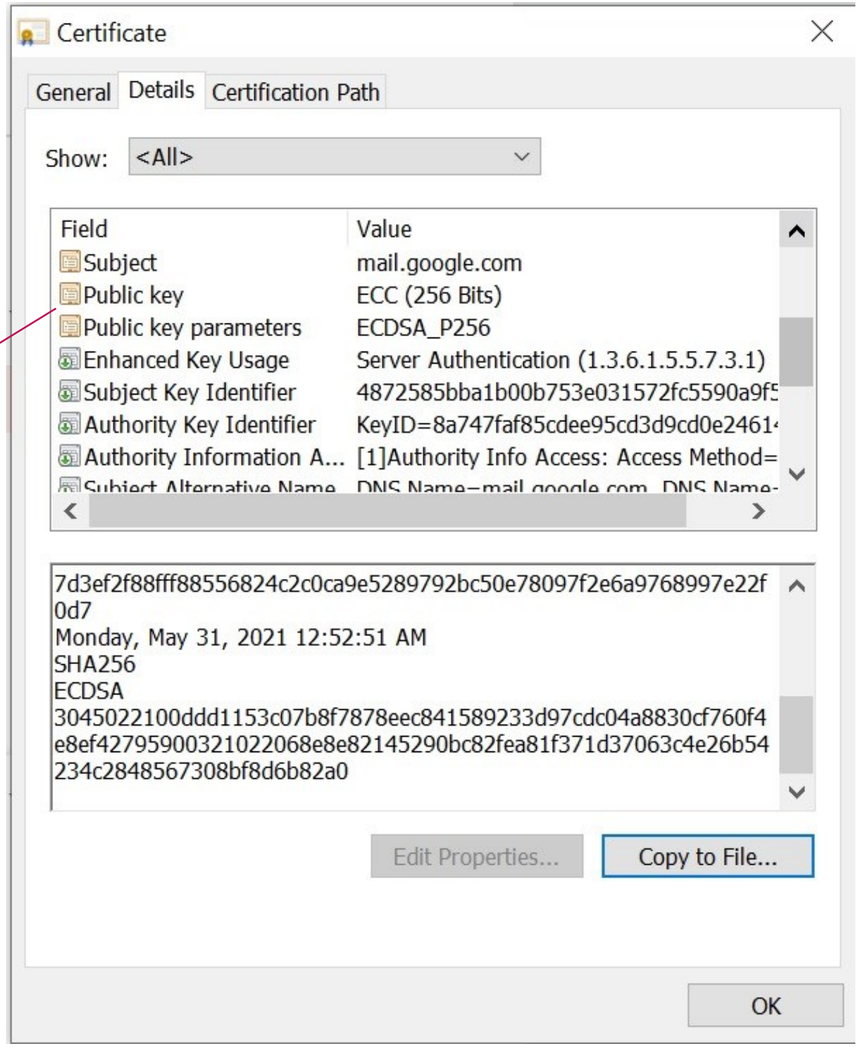
X.509 Components

Owner of public key

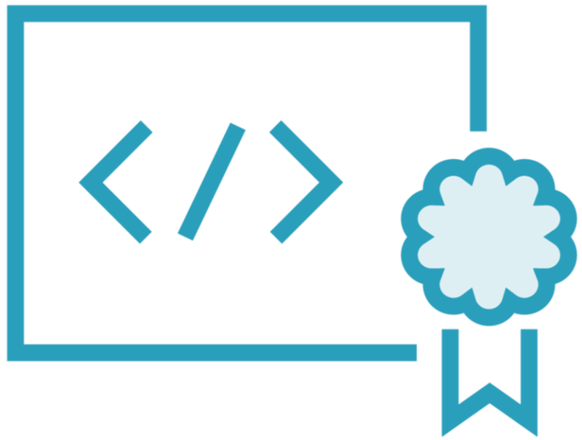


X.509 Components

Public key data

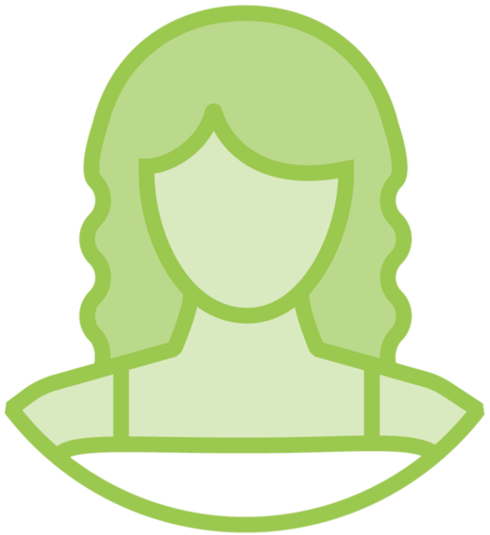


X.509 Four Names and Two Roles



Certificate Authority / Issuer

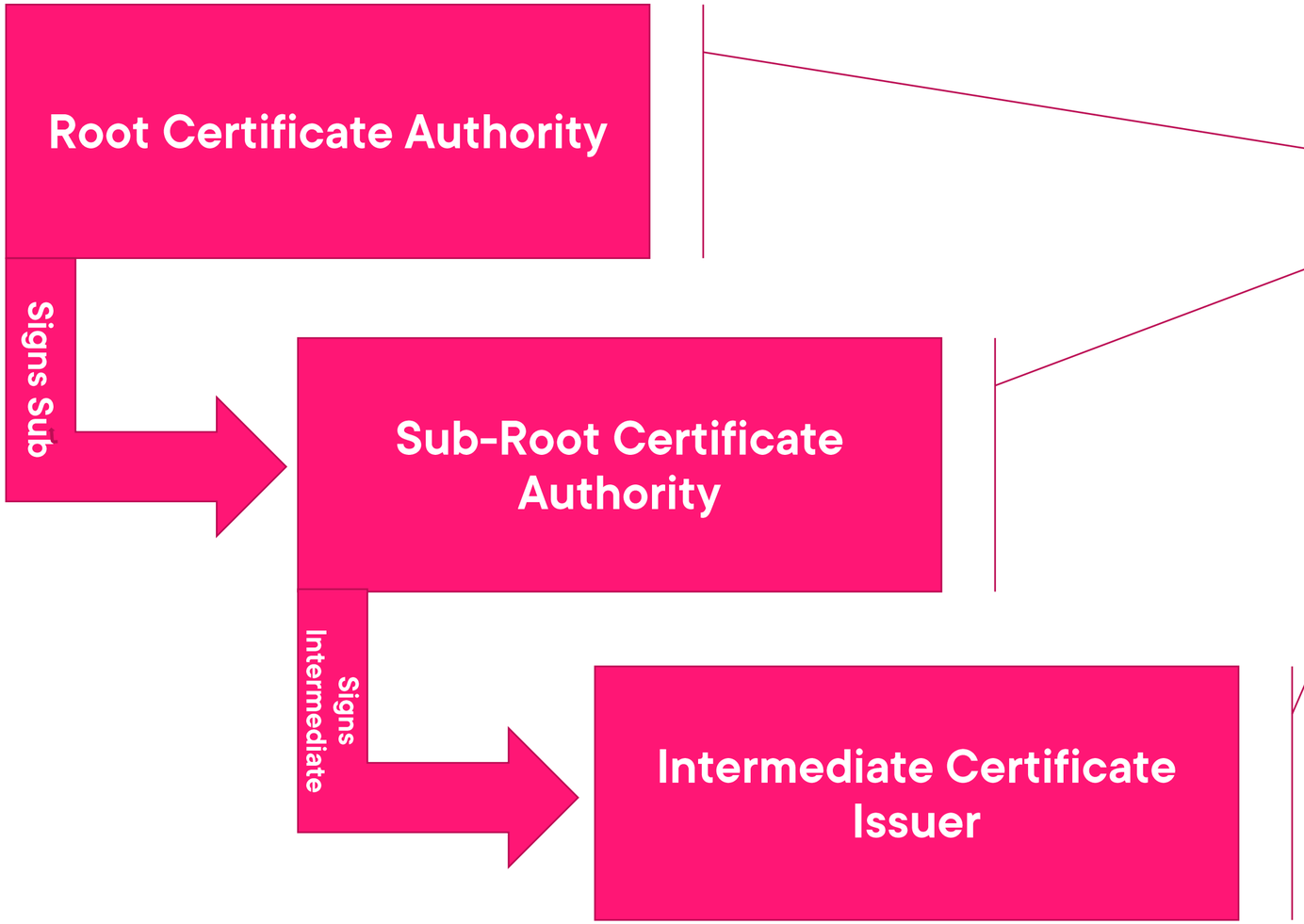
Signer of digital certificate by means of digital signature

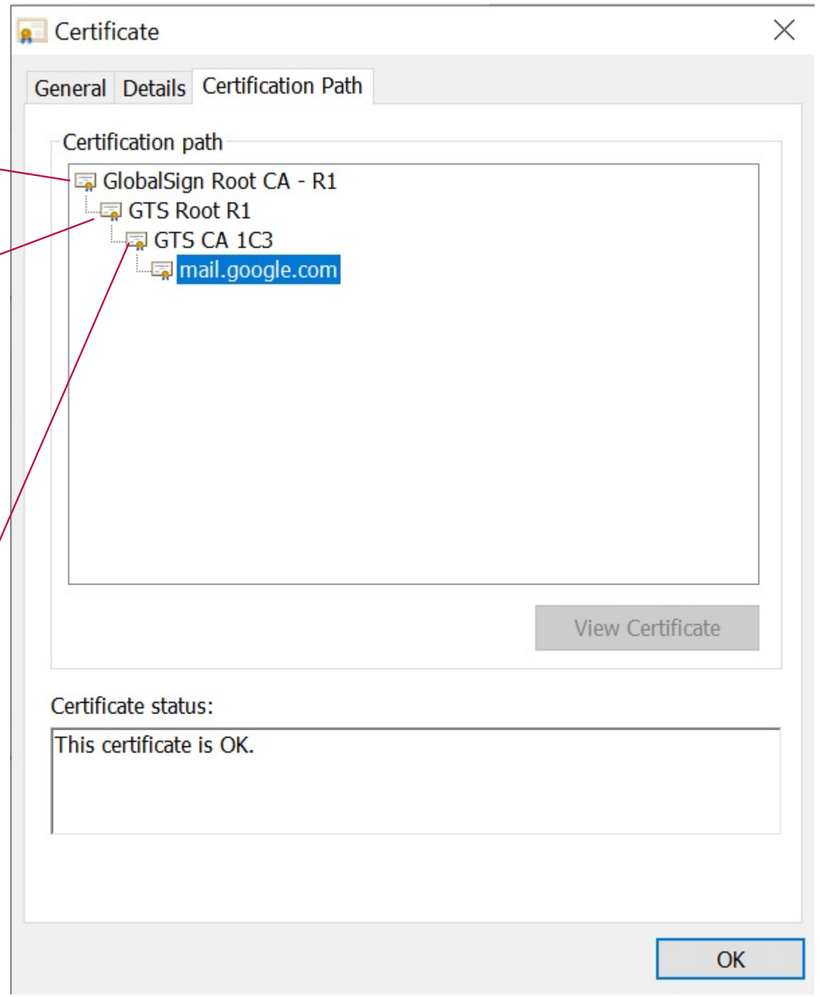


Subject / Owner

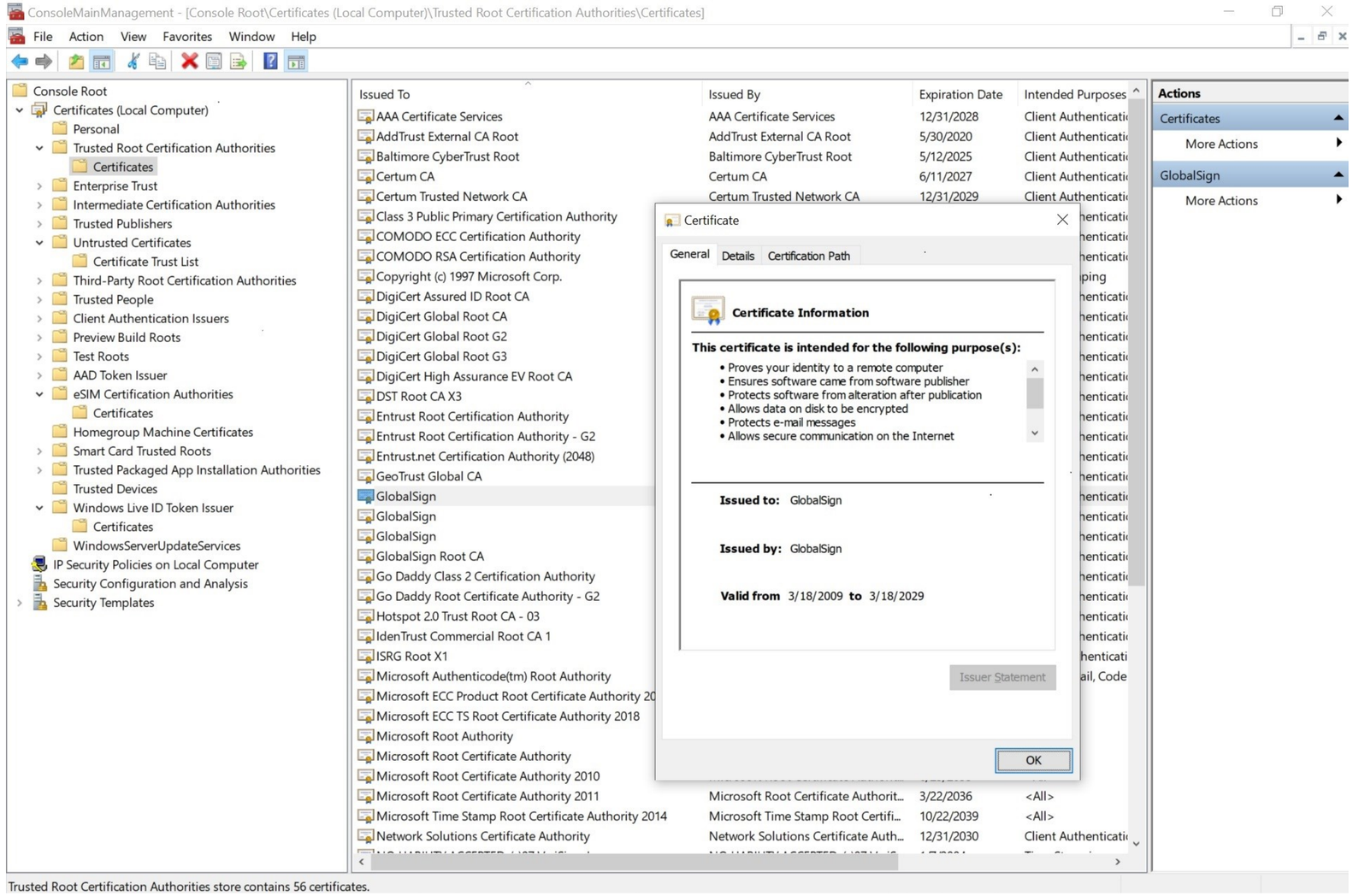
Authenticated public key bound to certificate of this entity

X.509 Hierarchical Chain of Trust





X.509 Local Trust Store



Types of X.509 certificates

Single domain

Multi-domain

Wildcard certificates

Multi-domain wildcard

Demo

Generate our own Certificate Signing Request (CSR) and then verify content

- This is the first technical step to being issued as X.509 certificate
- We will use Microsoft's Management Console with certificate add-on
- Then we will decode the request

Cryptanalysis and Limitations of Cryptography

Primary Cryptographic Attack Vectors

Frequency analysis	Password	Brute force
Social engineering	Algebraic	Implementation

Primary Cryptographic Attack Vectors

Rainbow table	Birthday	Dictionary
Replay	Factoring	Reverse engineering

Cryptanalysis Plaintext and Ciphertext

Ciphertext and Plaintext Attacks

Ciphertext-only

Known Plaintext

Chosen Plaintext

Chosen Ciphertext

Ciphertext-only Attack

Ciphertext

Bad actor

Ciphertext-only Attack

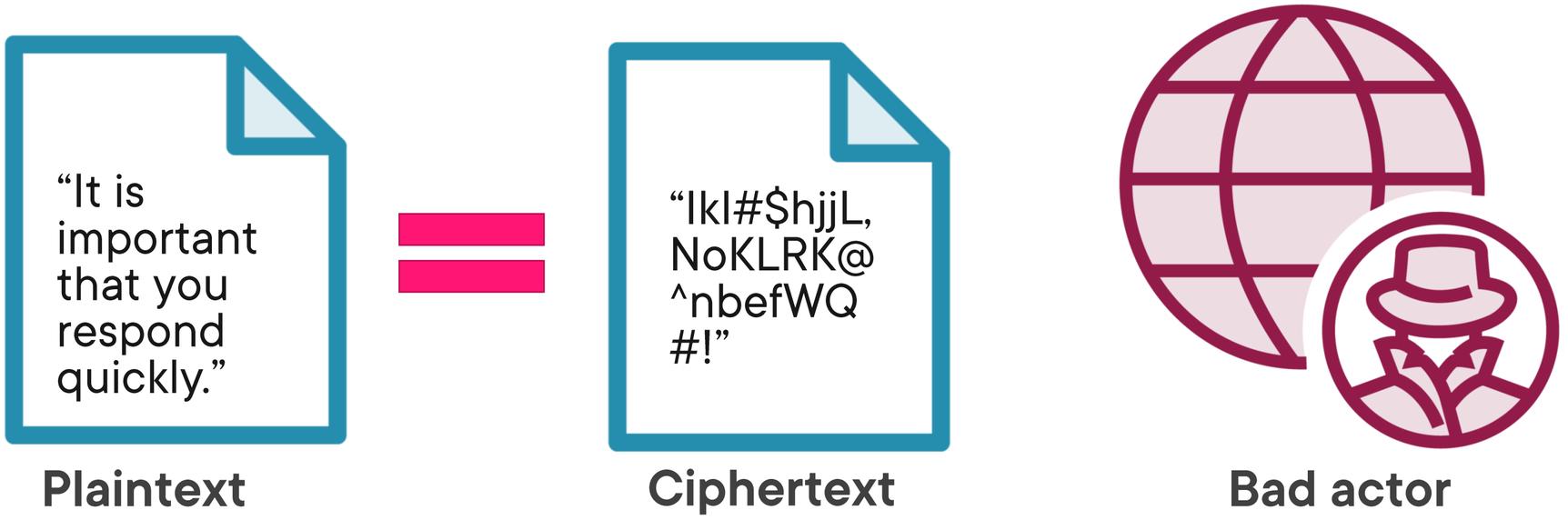
Known Plaintext Attack

Plaintext

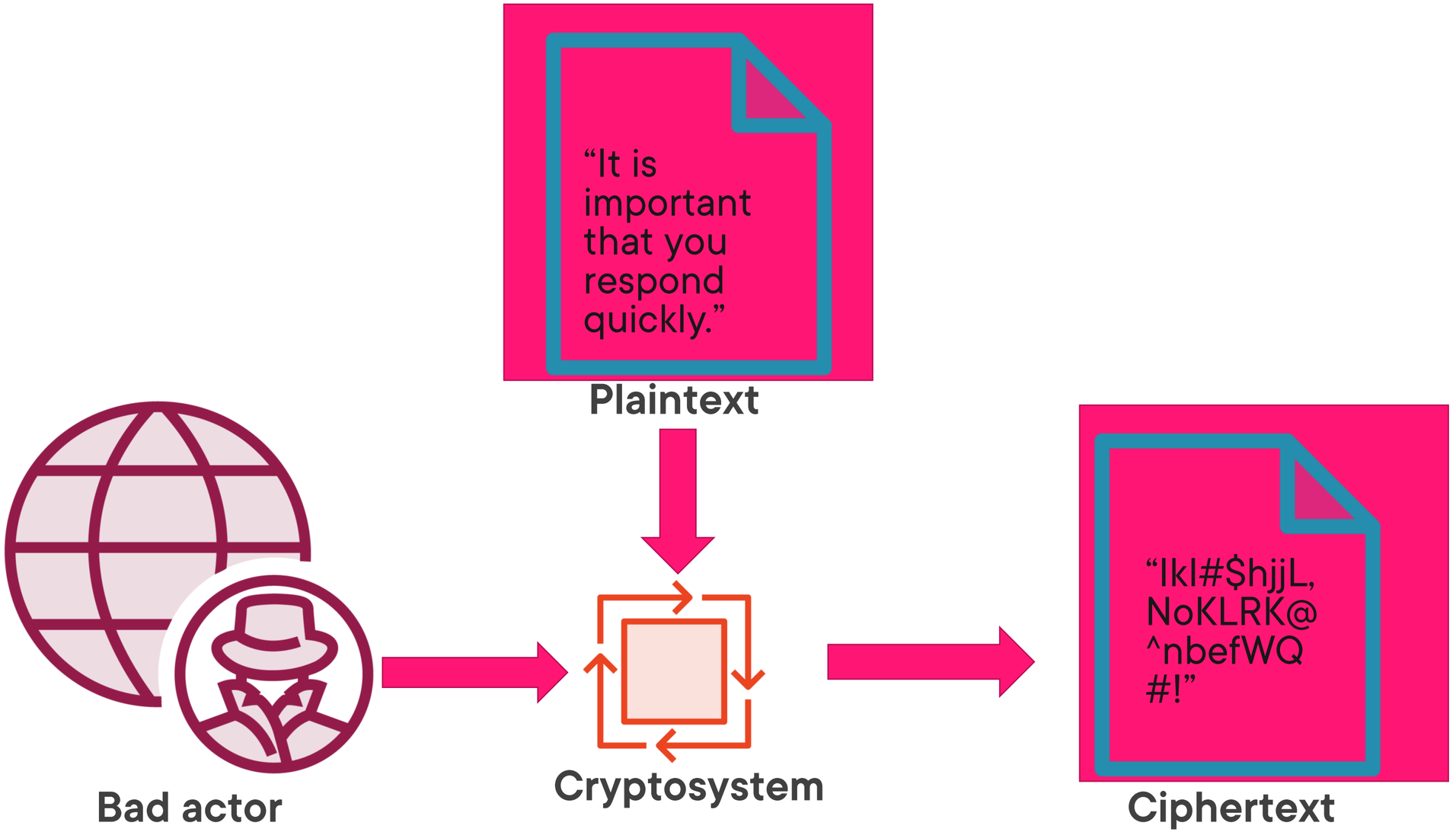
Ciphertext

Bad actor

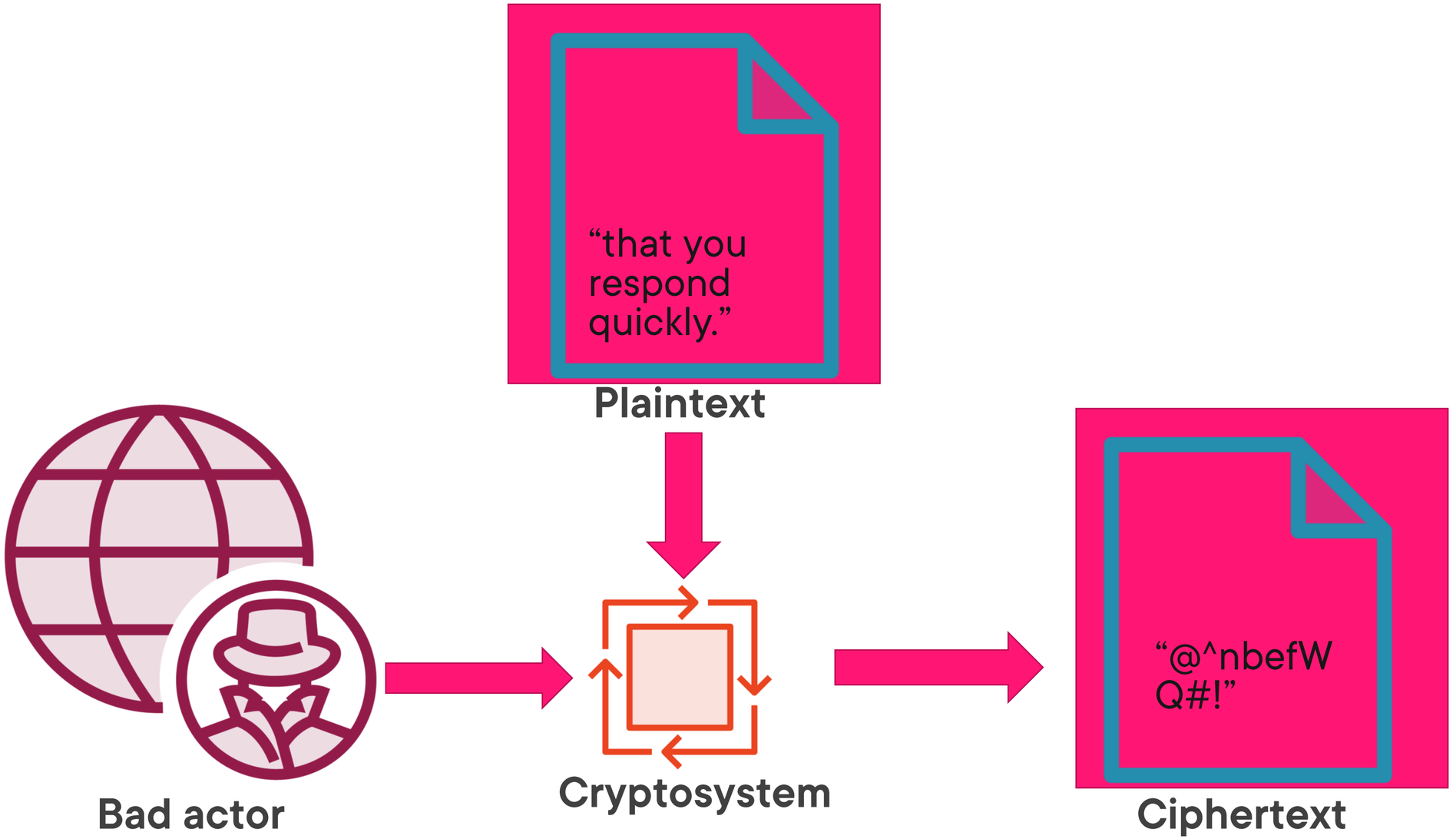
Known Plaintext Attack



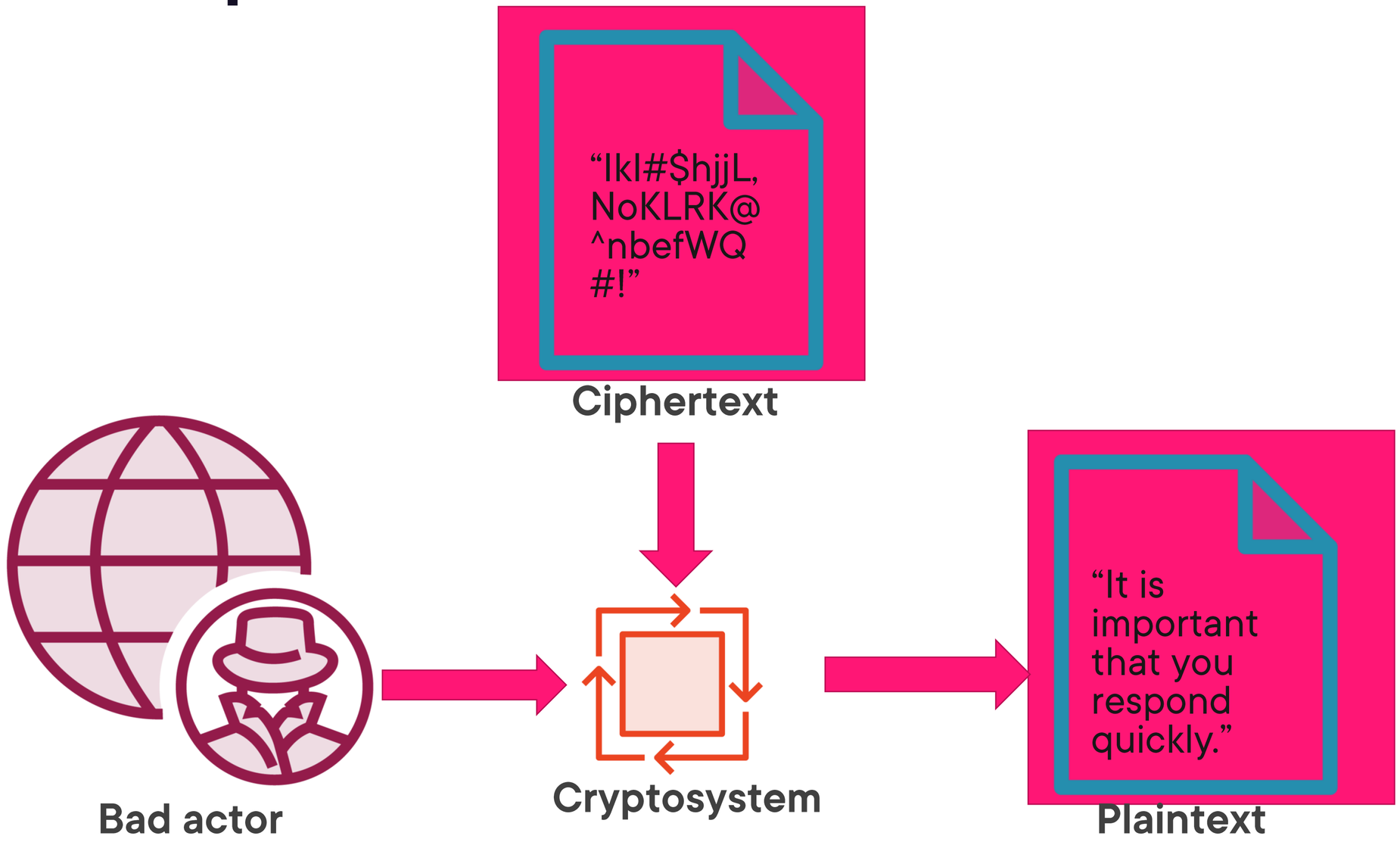
Chosen Plaintext Attack



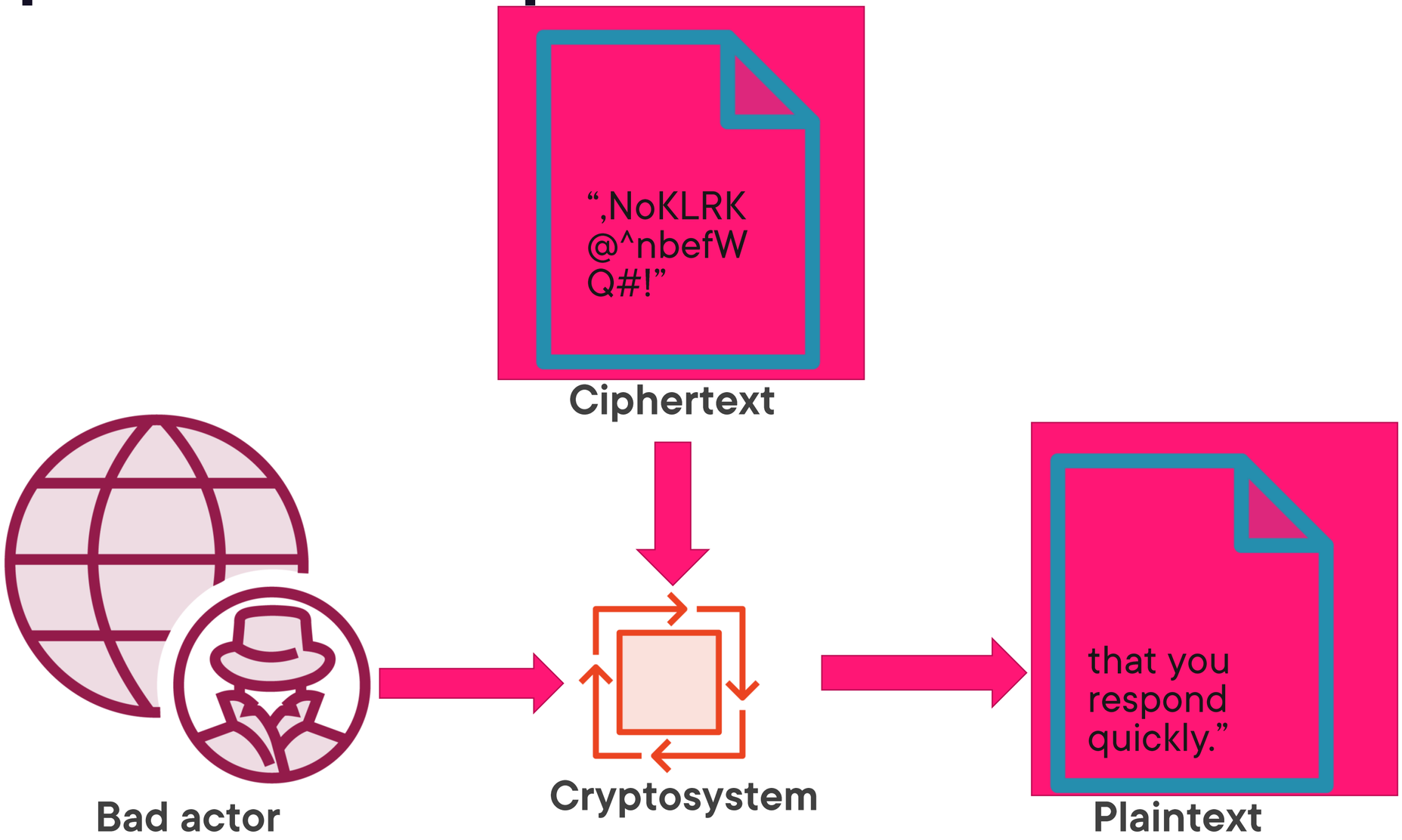
Adaptive Chosen Plaintext Attack



Chosen Ciphertext Attack

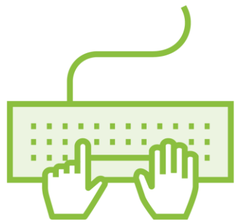


Adaptive Chosen Ciphertext Attack



Key Management Principles

Key Management Provisions

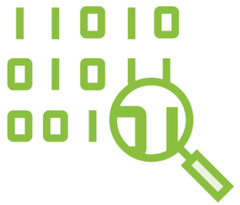


Policy management protocols

Crypto standards

Key length

Cryptoperiod lifecycle



Secure key generation

Separation of duties

Key Management Protocols

XML Key Management Specification 2.0:

- XML Key Information Service Specification (X-KISS)
- XML Key Registration Service Specification (X-KRSS)

ANSI X9.17

Secure Key Generation

Key creation

Automated generation

Pseudo-random and truly random

Separation of duties

Cryptoperiod Management

Shorter life is safer

Key escrow

Crypto-erasure necessary

Cryptograpic Standard

Federal Information Processing Standard (FIPS) 140-3

- Level 1
- Level 2
- Level 3
- Level 4

NIST SP 800-175B

Post-Quantum Cryptography Standards