

Secure Protocols and Cryptographic Lifecycles



Dr. Lyron H. Andrews

Cryptography for SSCP®

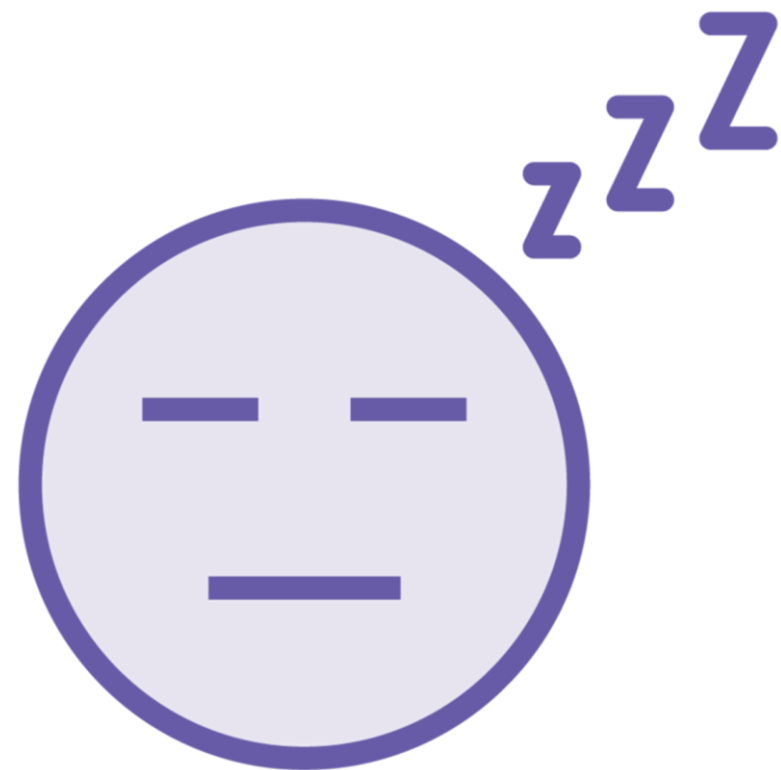
@drlyronandrews | www.profabula.com



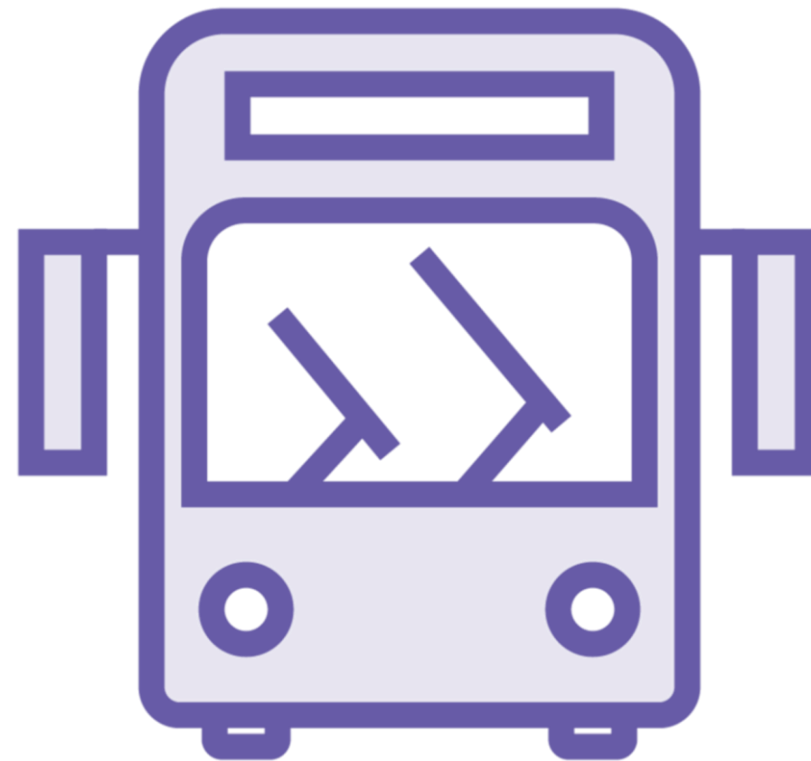
Cryptographic Implementation and Use Cases



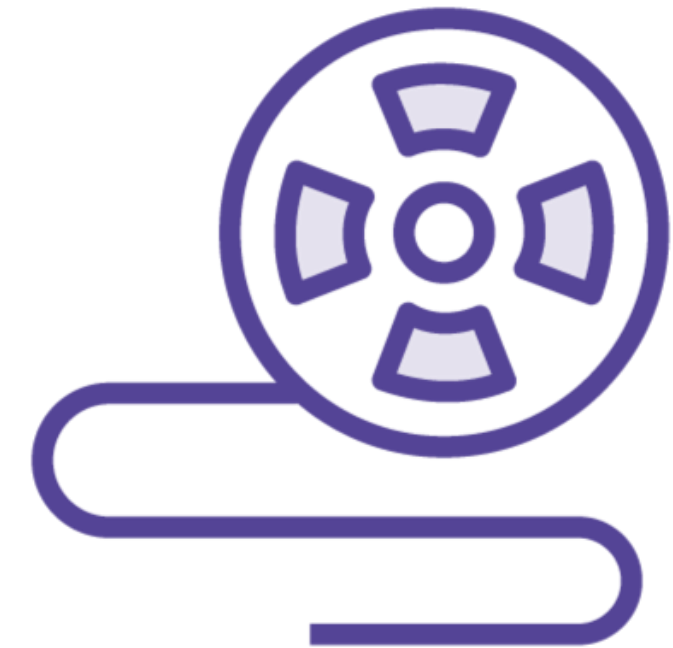
Three States of Data



Data at rest
Storage systems



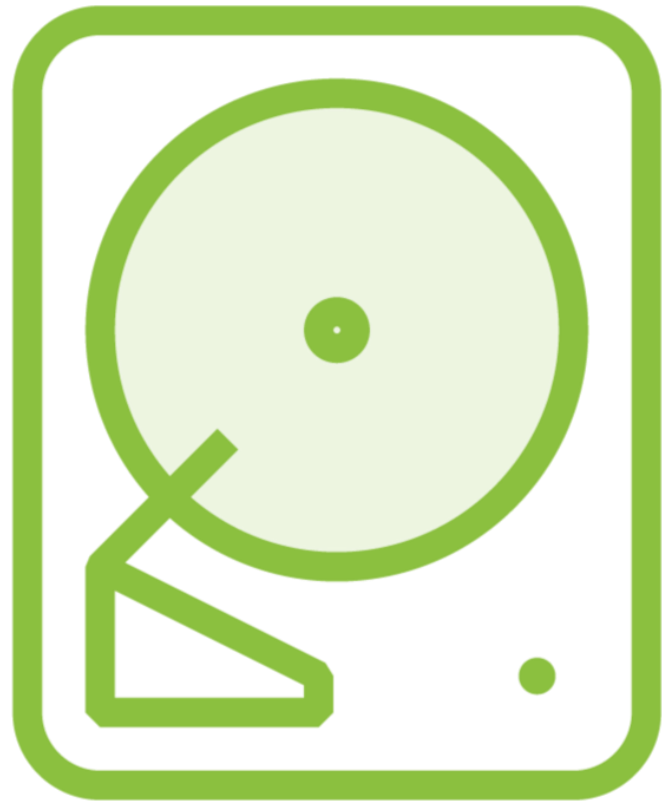
Data in transit
Moving locations



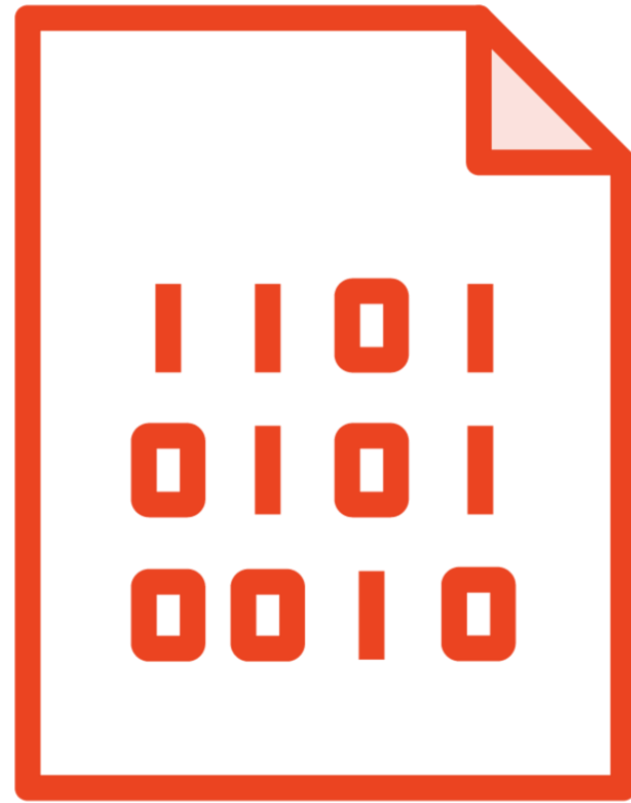
Data in use
Interaction with
systems/people



Primary Use Cases



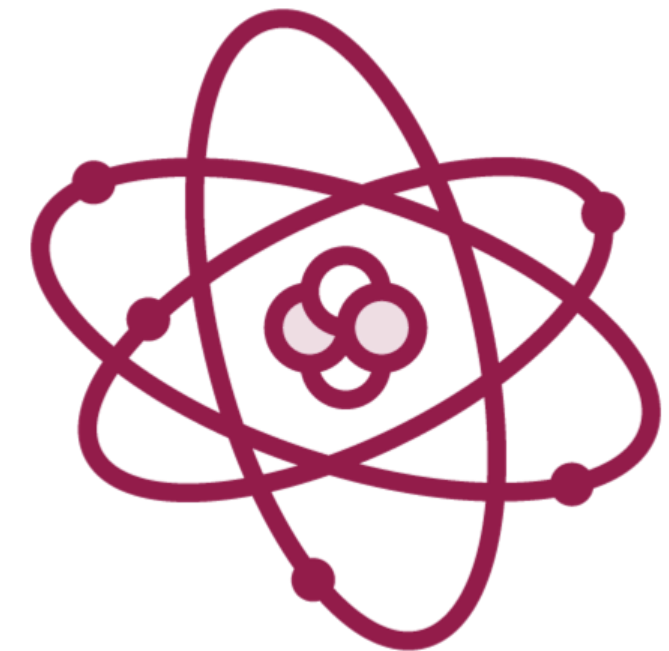
Disk encryption



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)

ESP header

ESP payload

ESP trailer

Authentication



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

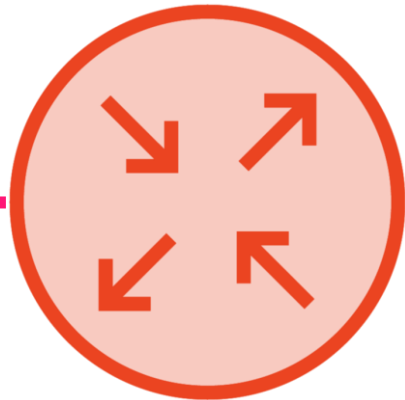
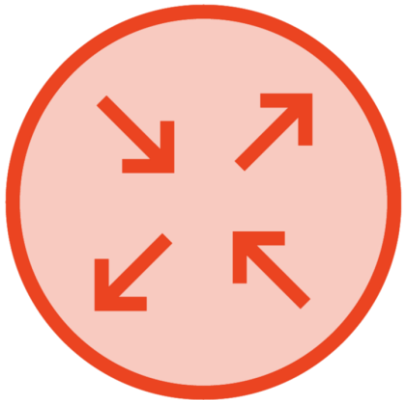


IPSEC Transport and Tunnel Mode

Network A

When concerned about surveillance between network A and B

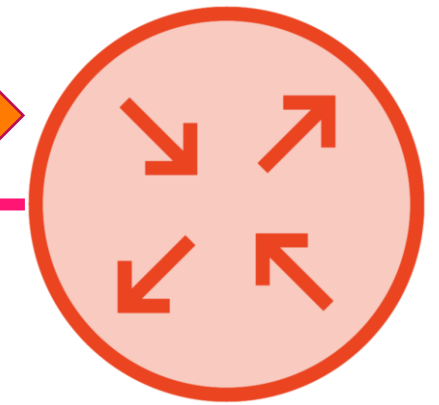
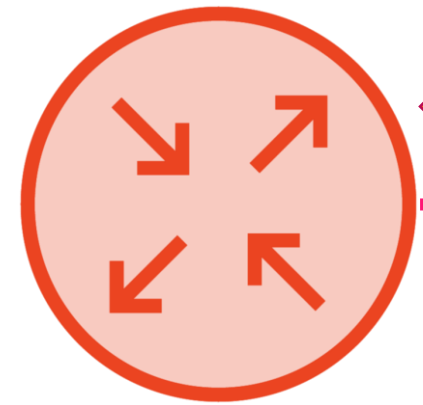
Network B



IPSEC Transport and Tunnel Mode

Network A

Network B



Link Encryption or Tunnel Mode



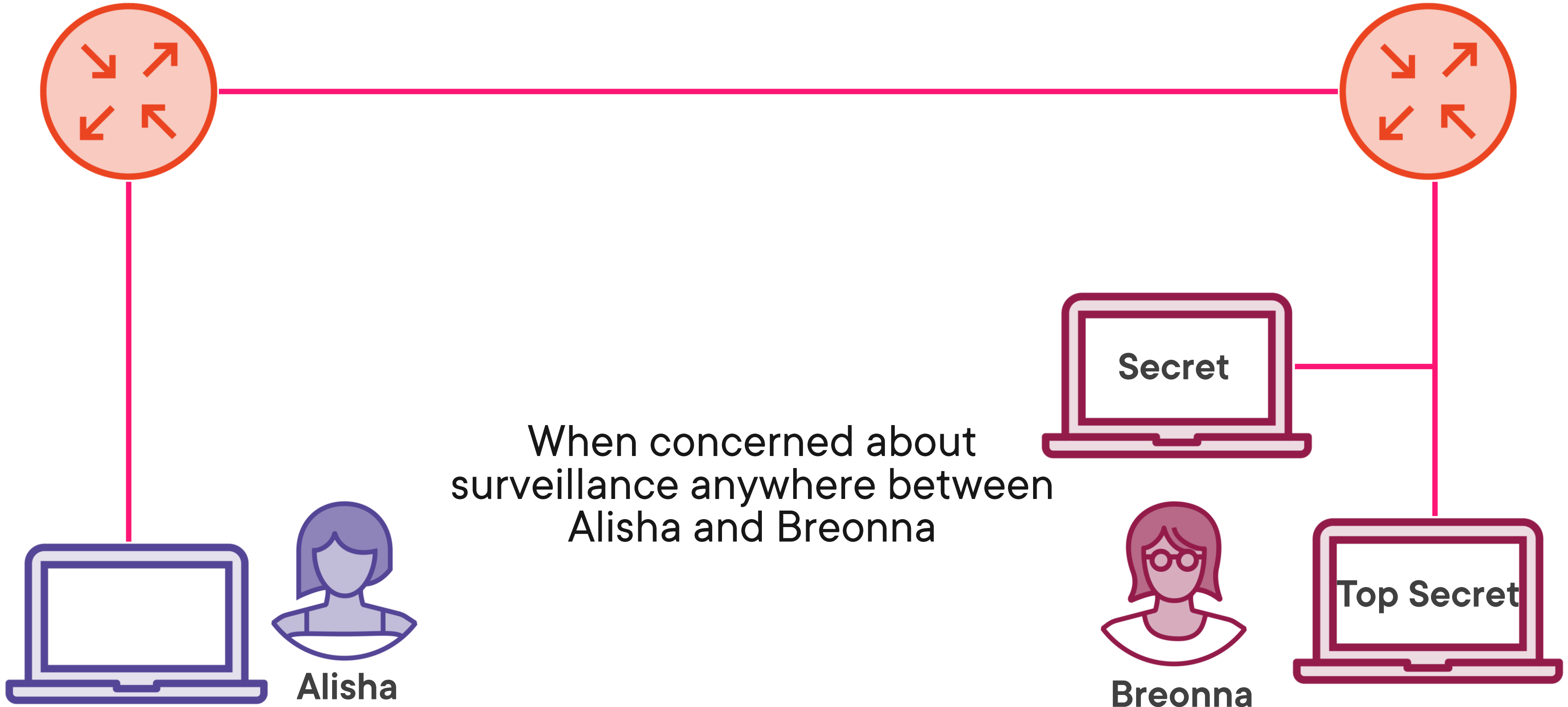
When concerned about surveillance
between network A and B



IPSEC Transport and Tunnel Mode

Network A

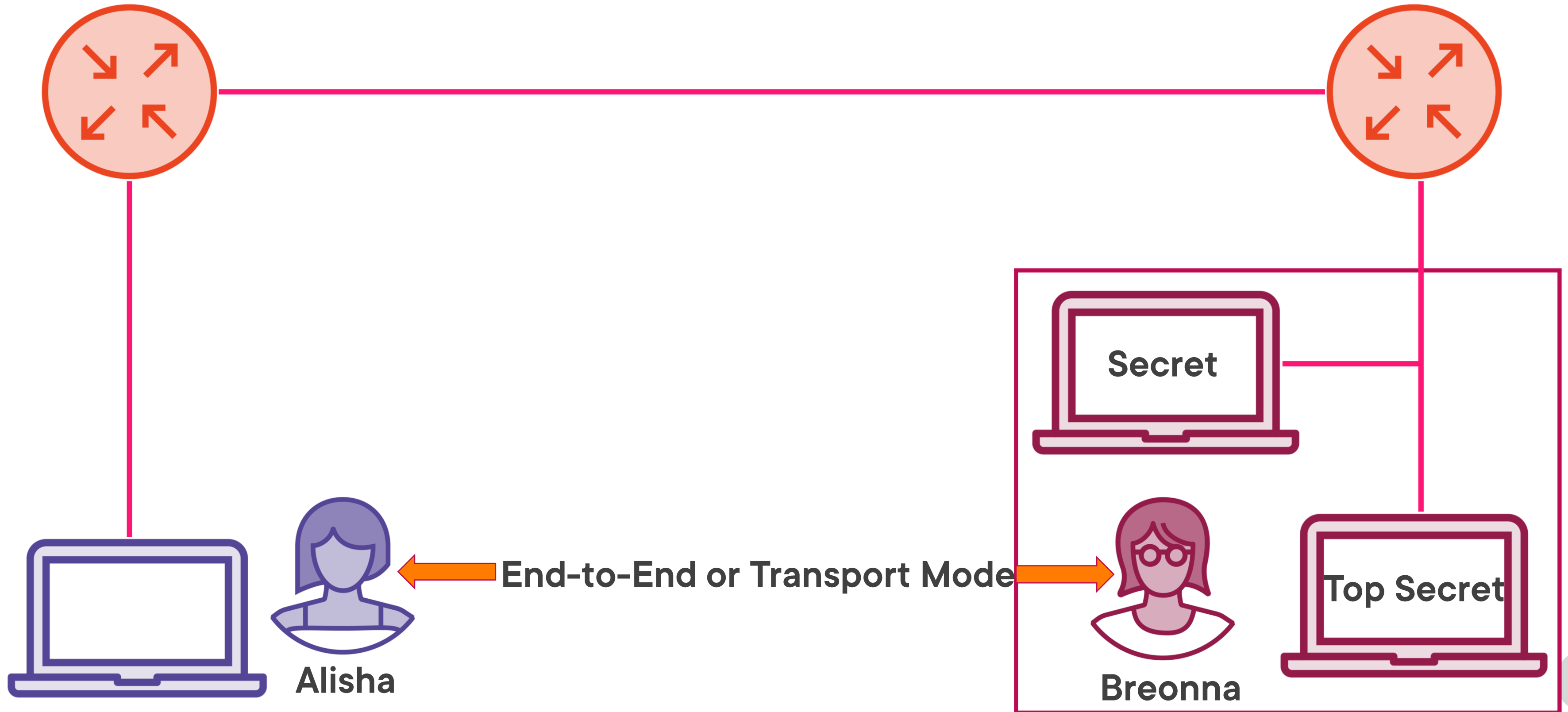
Network B



IPSEC Transport and Tunnel Mode

Network A

Network B



Cryptographic Protocols and Services – Transport Layer Security (TLS)

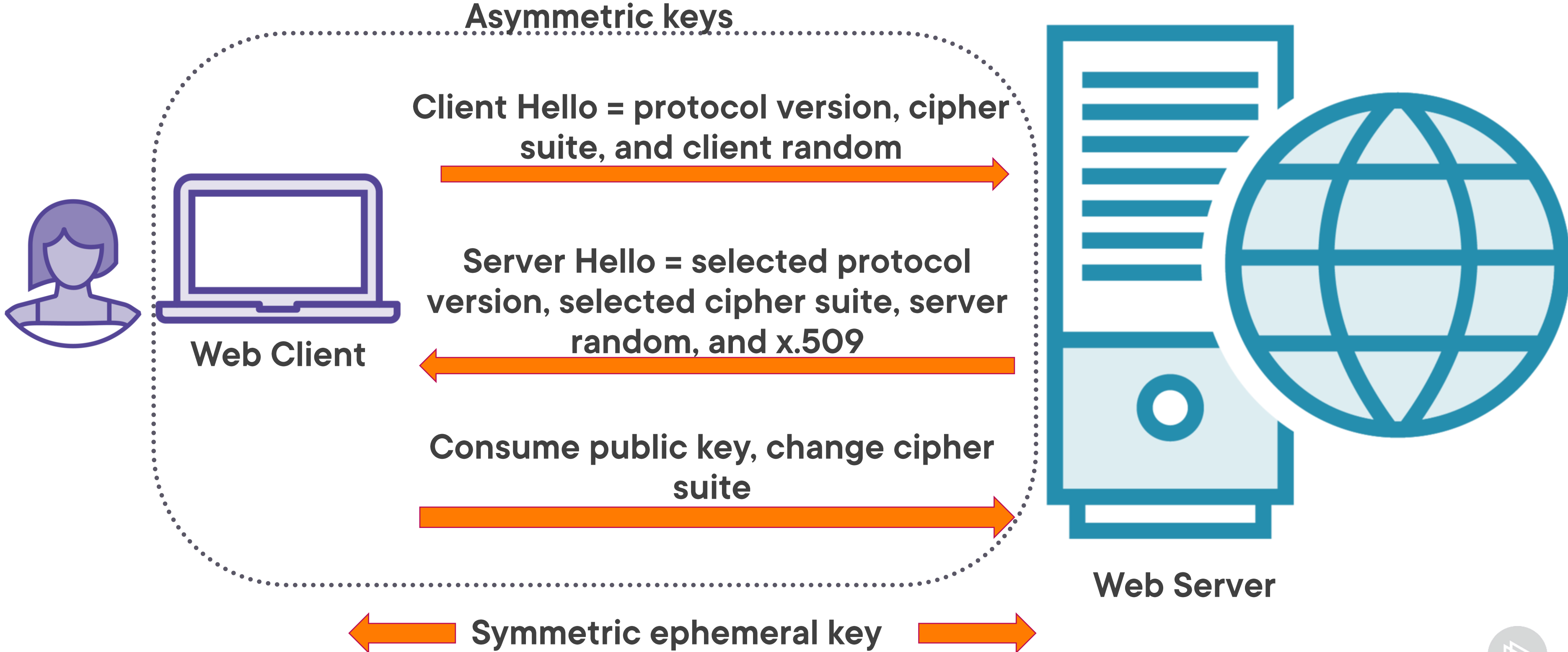


Started as SSL 2.0
TLS 1.0 and SSL 3.0
TLS 1.1, 1.2, and 1.3

History of SSL/TLS



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



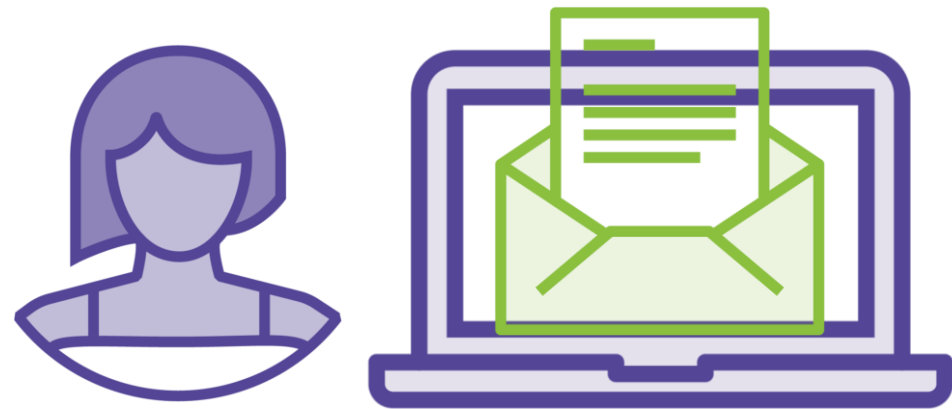
Prove sender identity



Maintain message integrity



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



Alisha



Breonna



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



Alisha



Breonna



Alisha's private key



Digitally signs message



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



Alisha



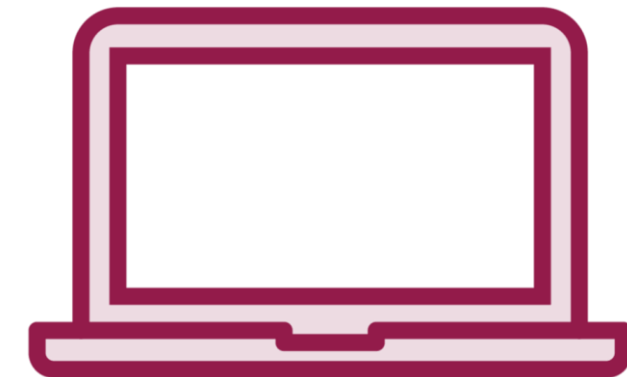
Breonna's
public key



Alisha's
private key



Digitally signs
message



Breonna



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



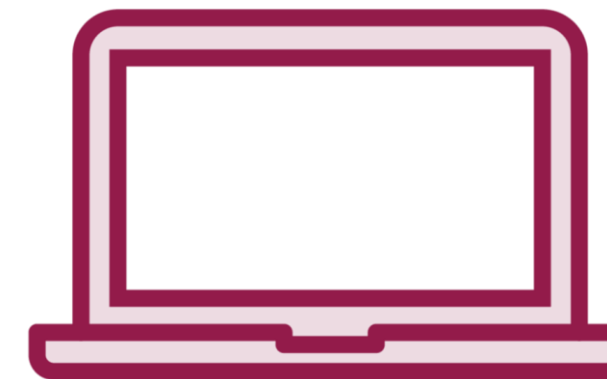
Alisha



Breonna's
public key



Encrypts the
message



Breonna



Alisha's
private key



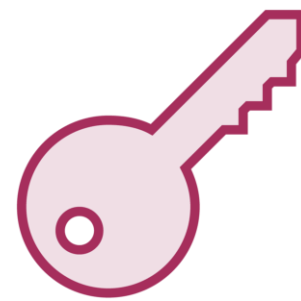
Digitally signs
message



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



Alisha



Breonna's private key



Decrypts the message



Breonna



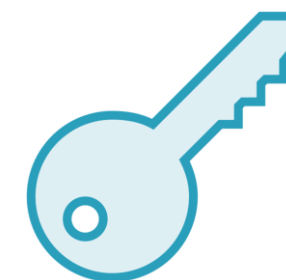
Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities



Alisha



Breonna



Alisha's public key



Verifies sender



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



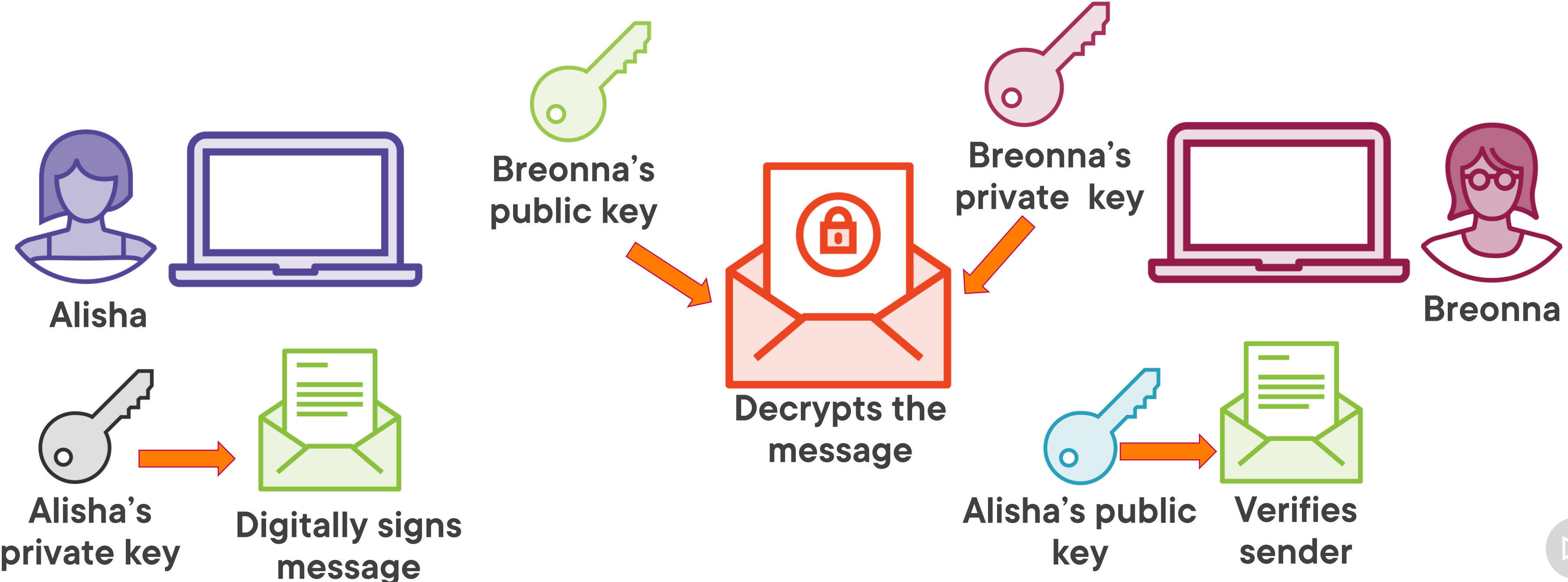
Alisha



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-originating 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.



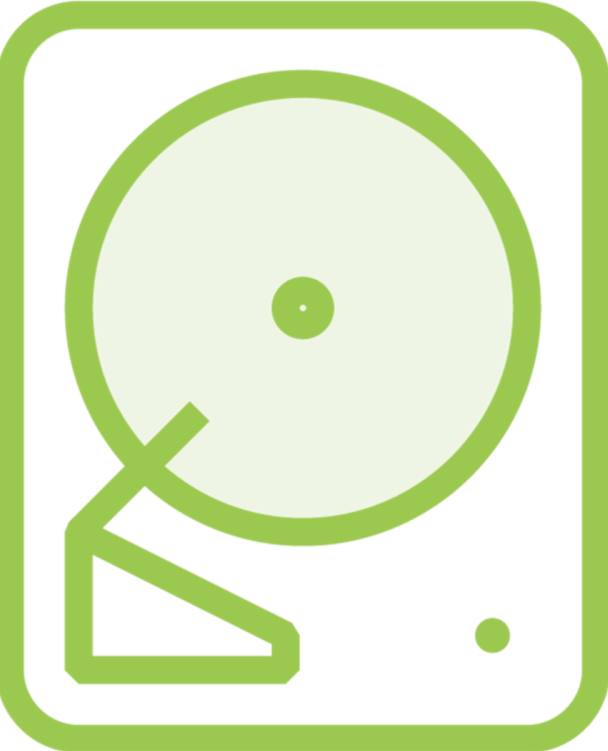
Disk and File Encryption Use Cases



Full Disk Encryption



Symmetric key
encrypts data



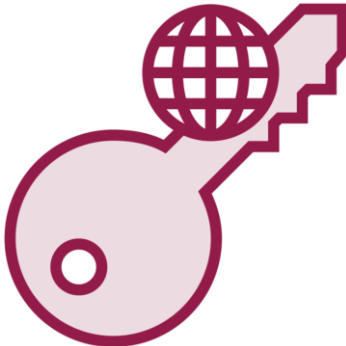
Volume



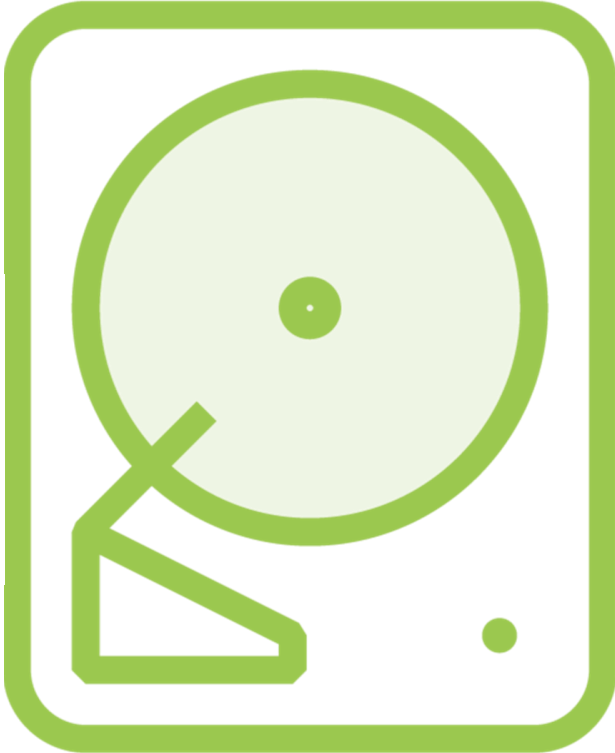
Full Disk Encryption



Public or symmetric key encrypts volume key



Symmetric volume key encrypts data



Volume

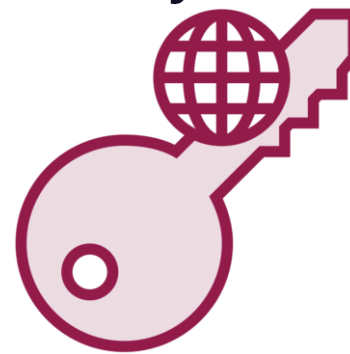


Full Disk Encryption

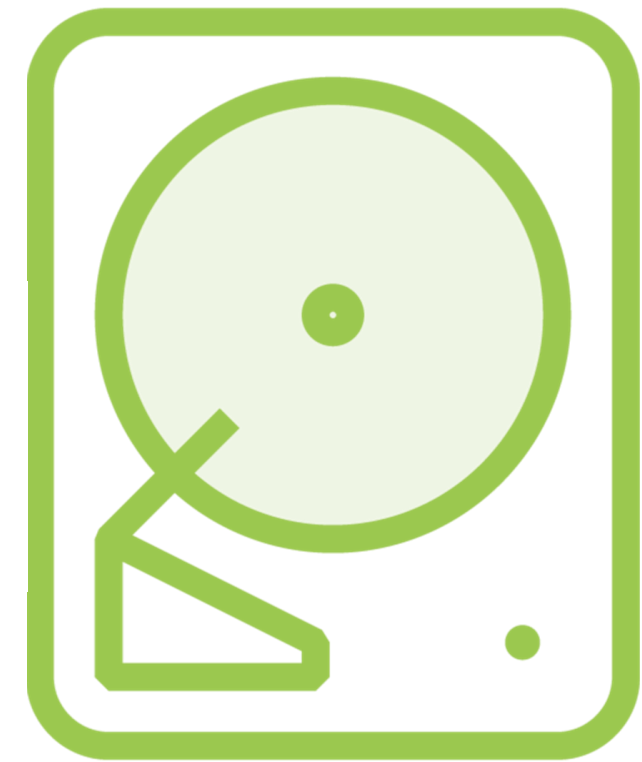


TPM or user
private key
decrypts
public

Public or
symmetric key
encrypts
volume key



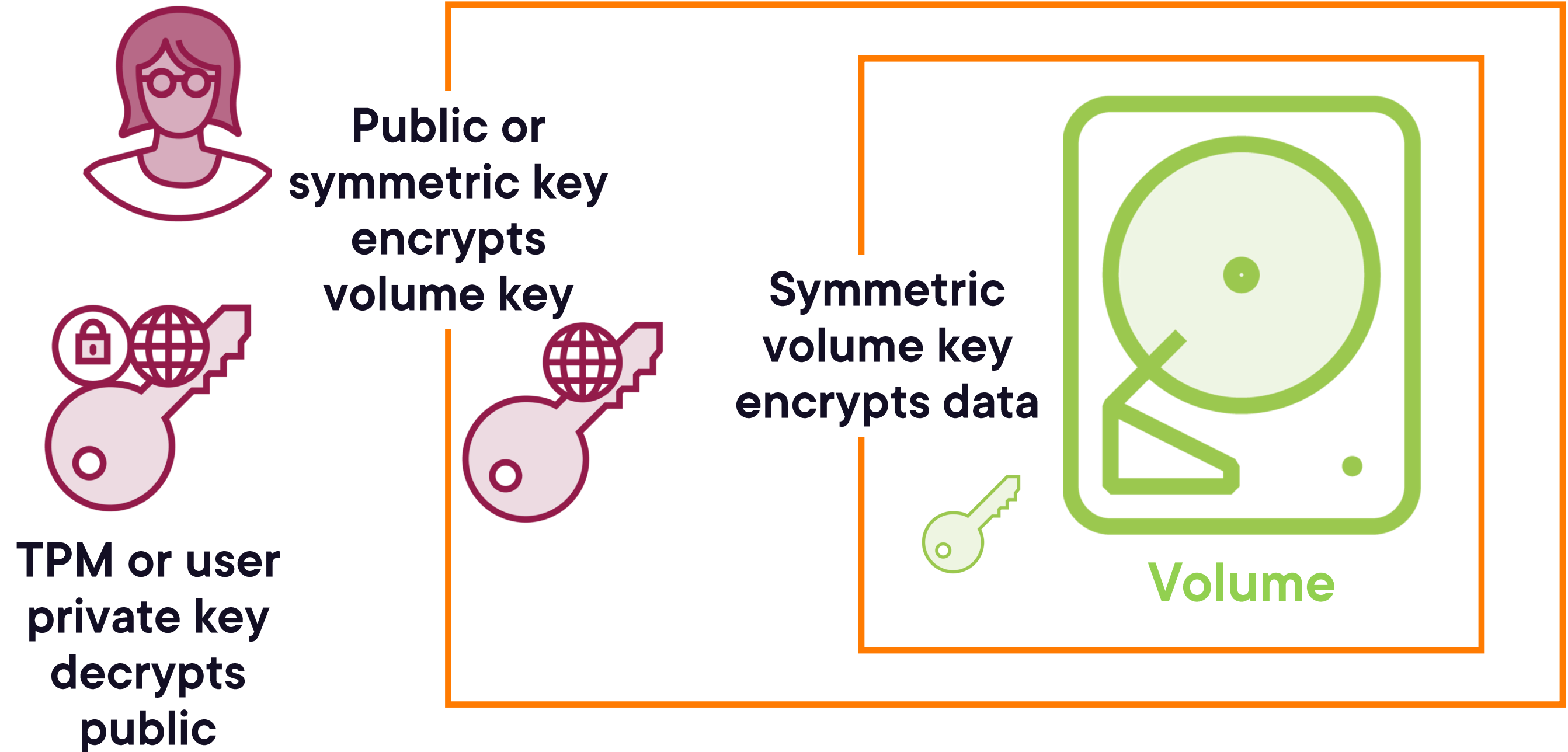
Symmetric
volume key
encrypts data



Volume



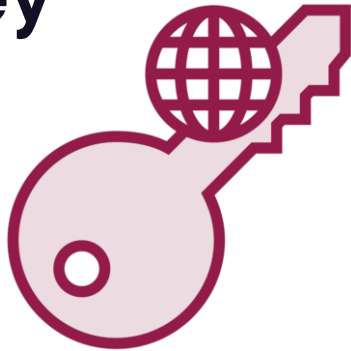
Full Disk Encryption



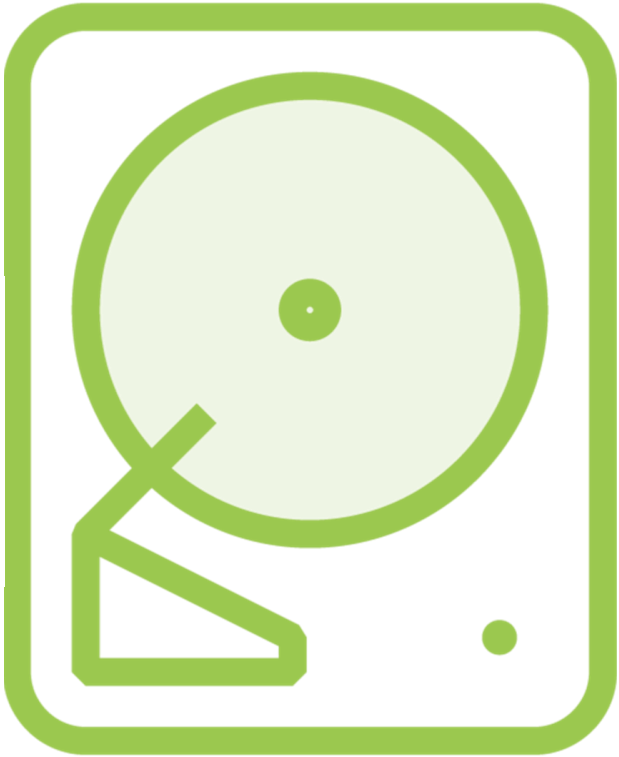
Full Disk Encryption



Public or symmetric key decrypts volume key



Symmetric volume key encrypts data



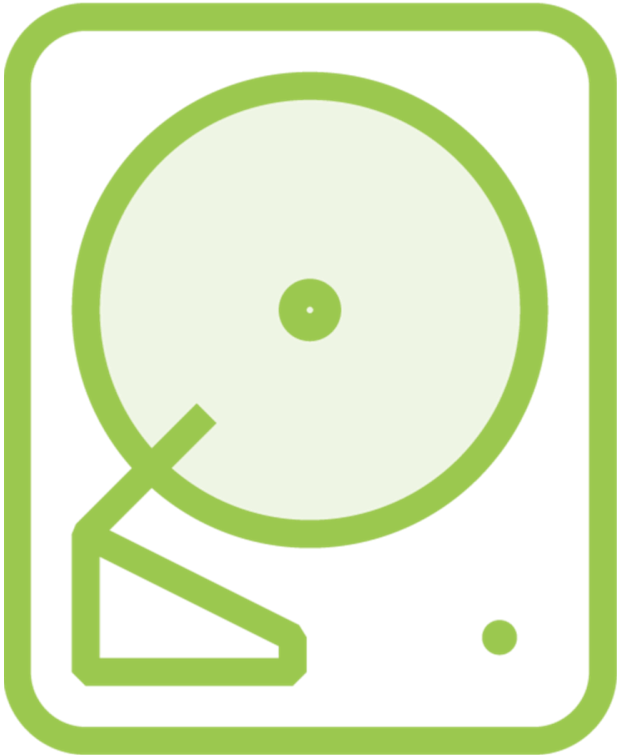
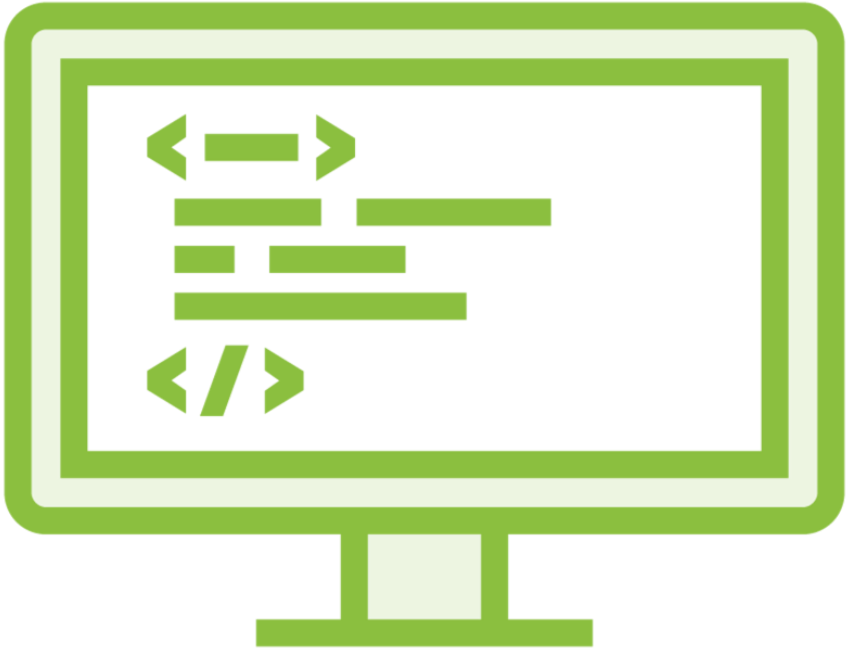
Volume



Full Disk Encryption



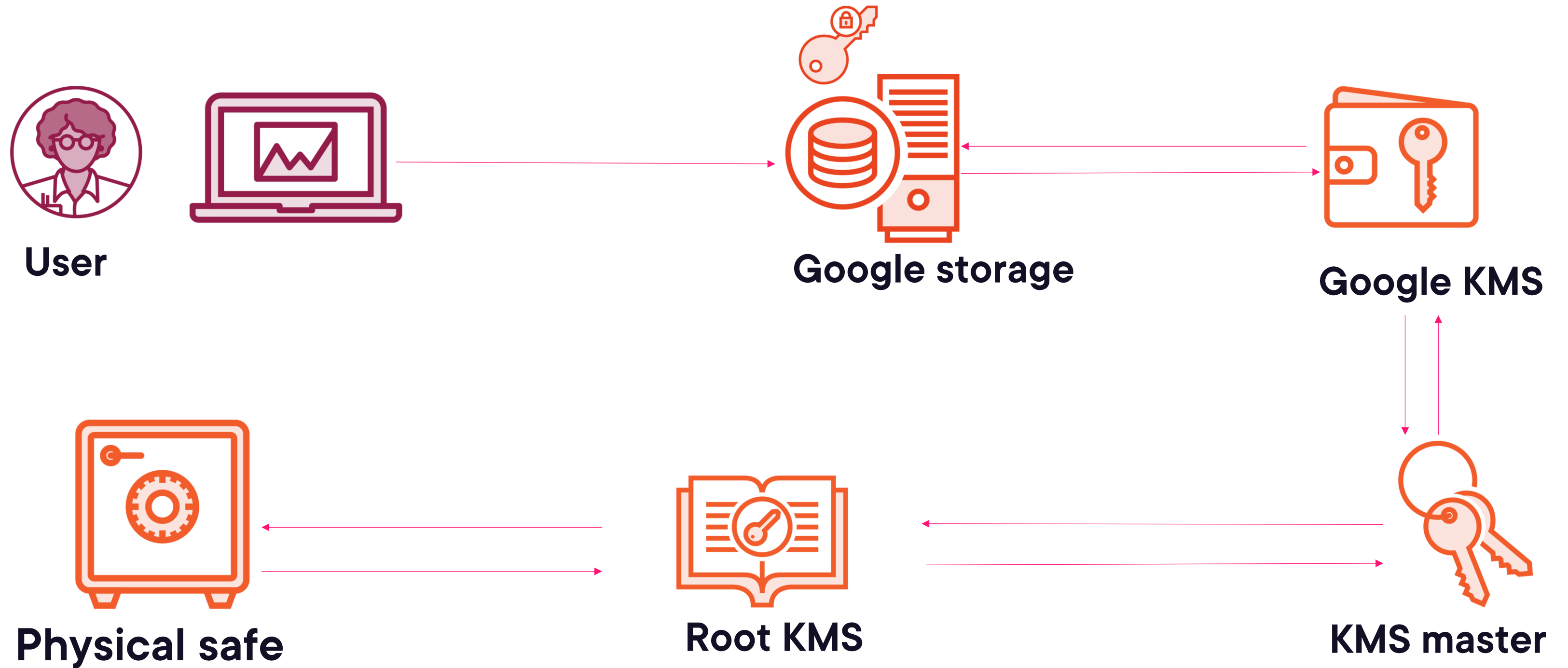
User access to resource granted



Volume



Google Key Wrapping



Public Key Infrastructure Principles



Pretty Good Privacy

Three things that you need to know

1

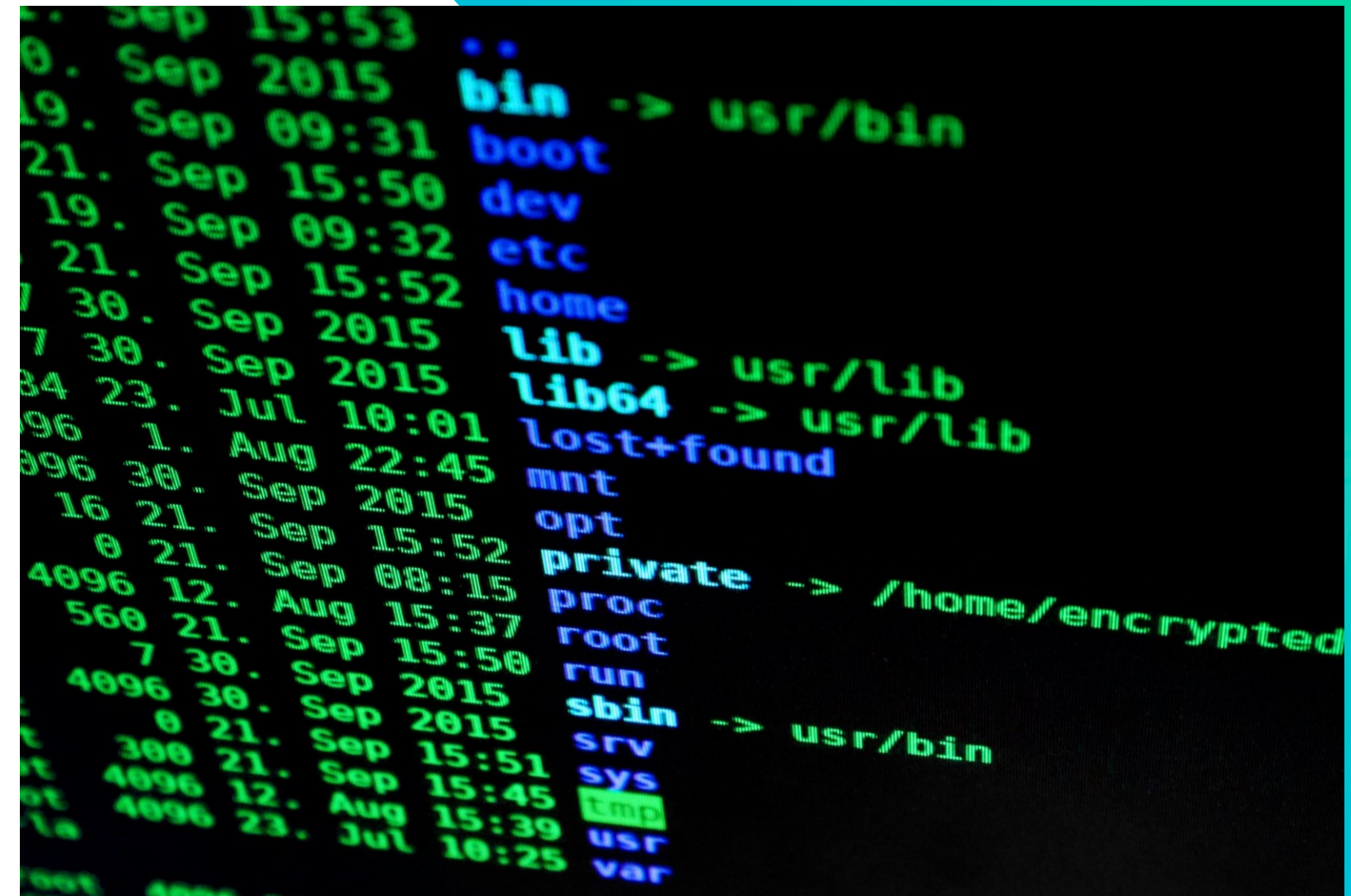
Public-private key pair algorithm developed in 1991 by Phil Zimmerman

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



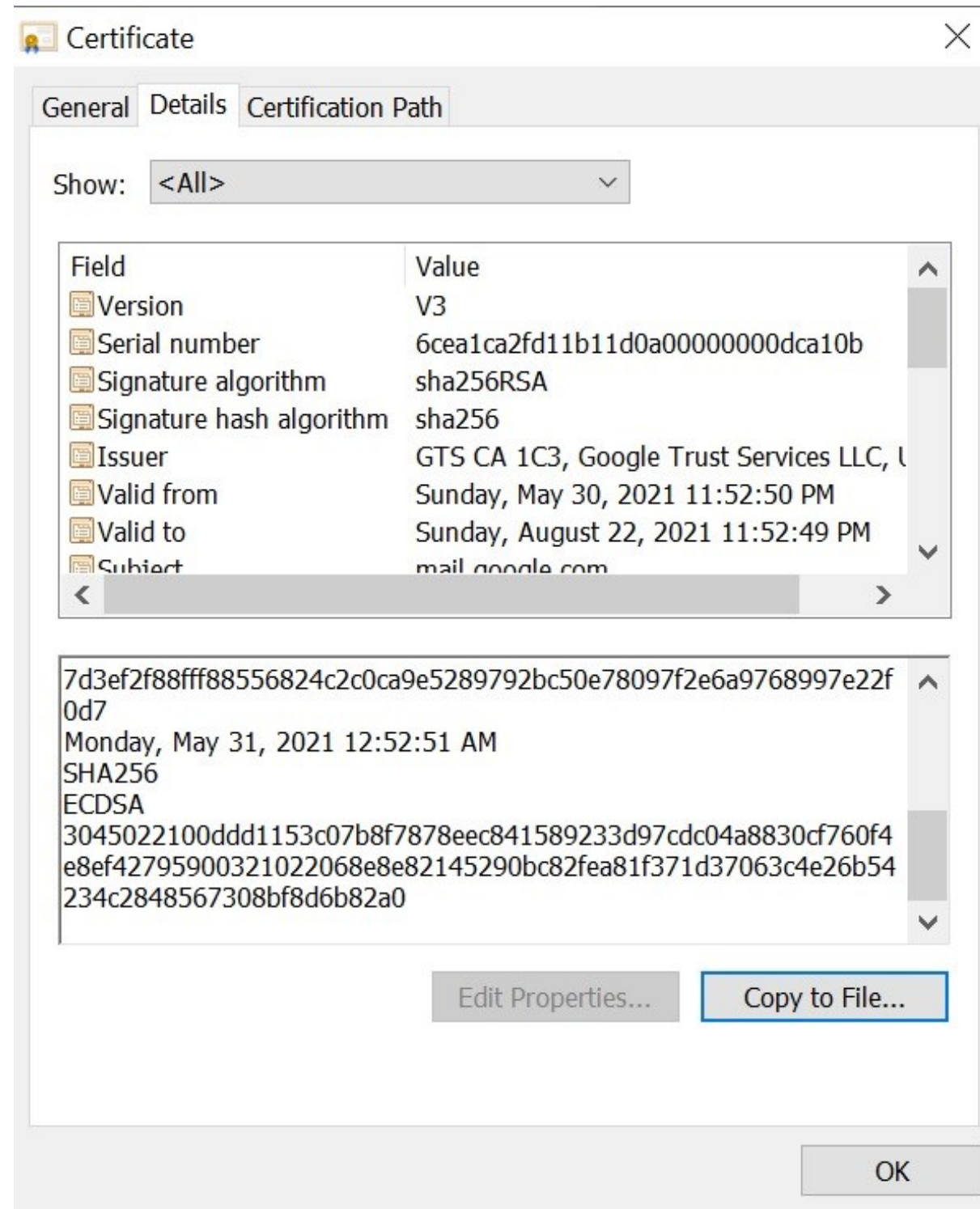
Attestation of entities, trust, and assurance



Confidentiality of communication channels

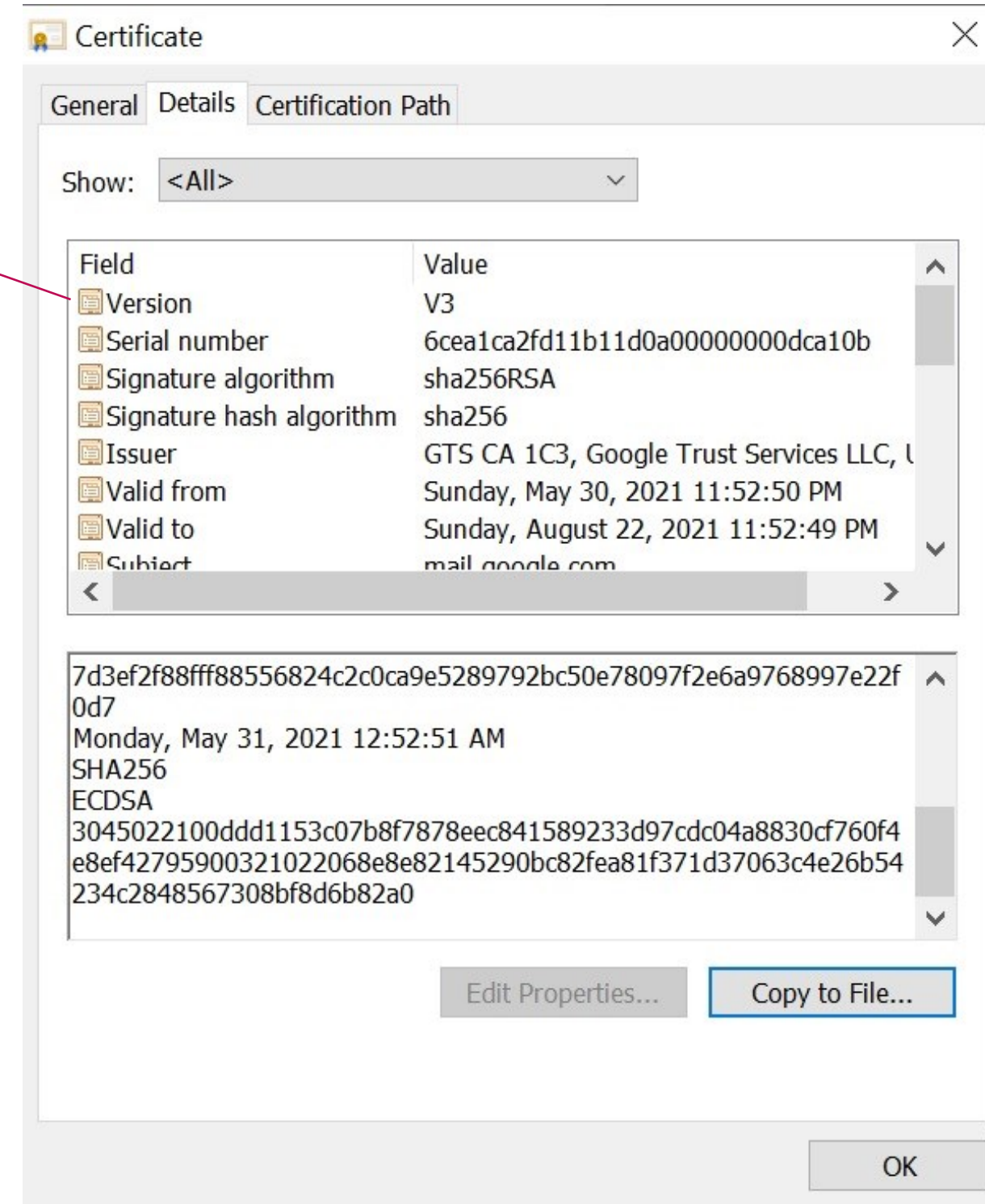


X.509 Components



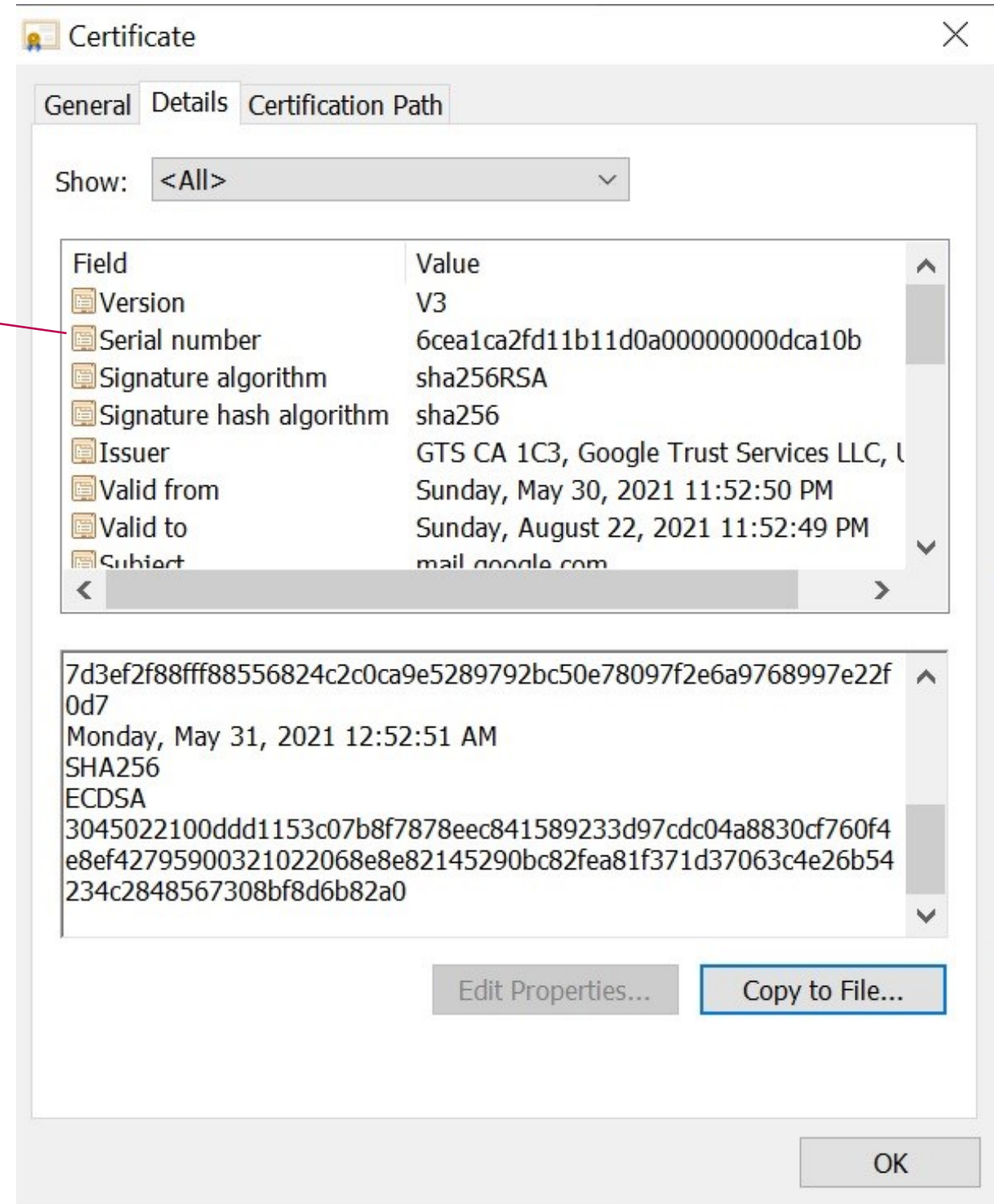
X.509 Components

Version of certificate



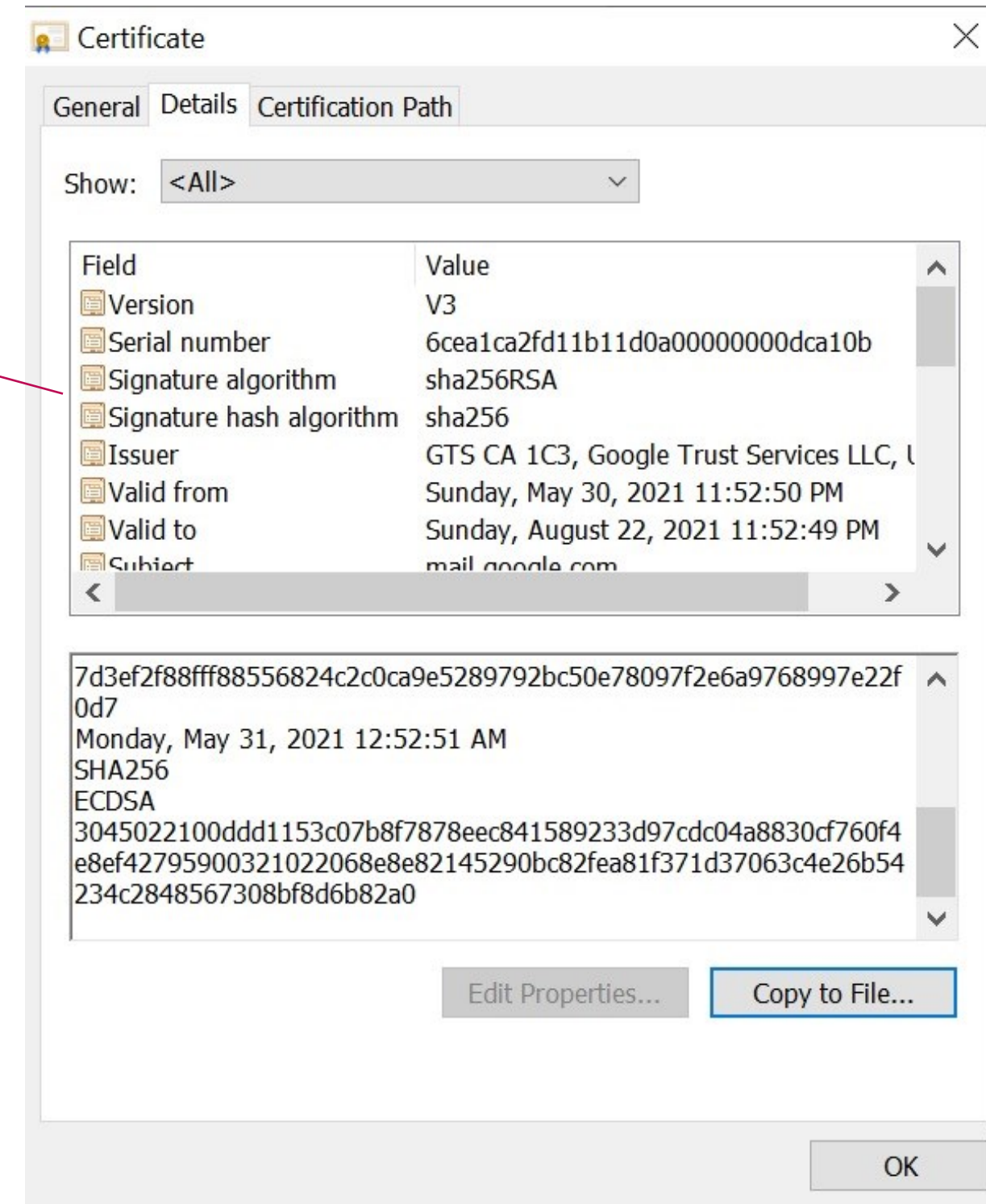
X.509 Components

Positive unique integer



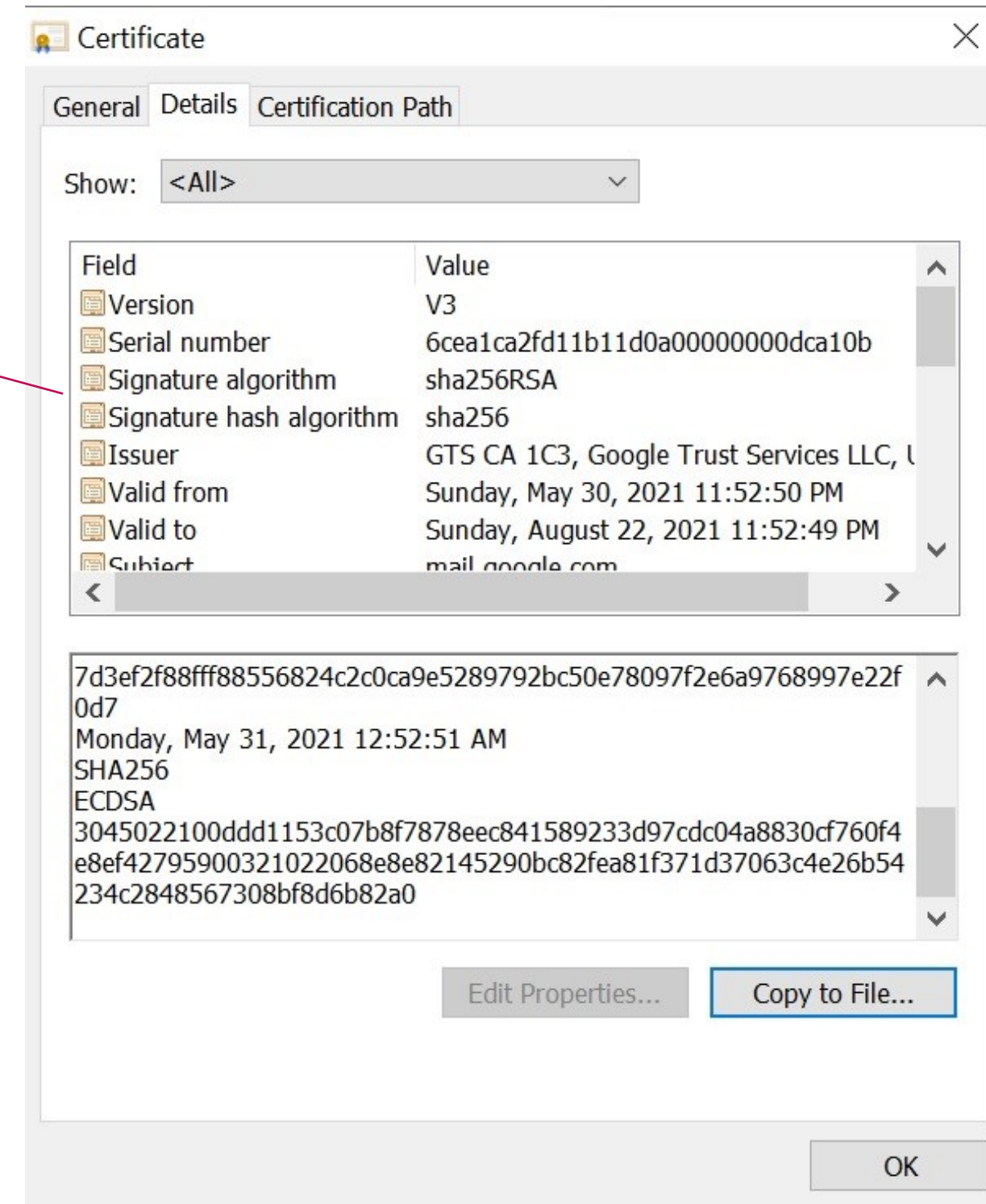
X.509 Components

Algorithm used by CA to sign certificate



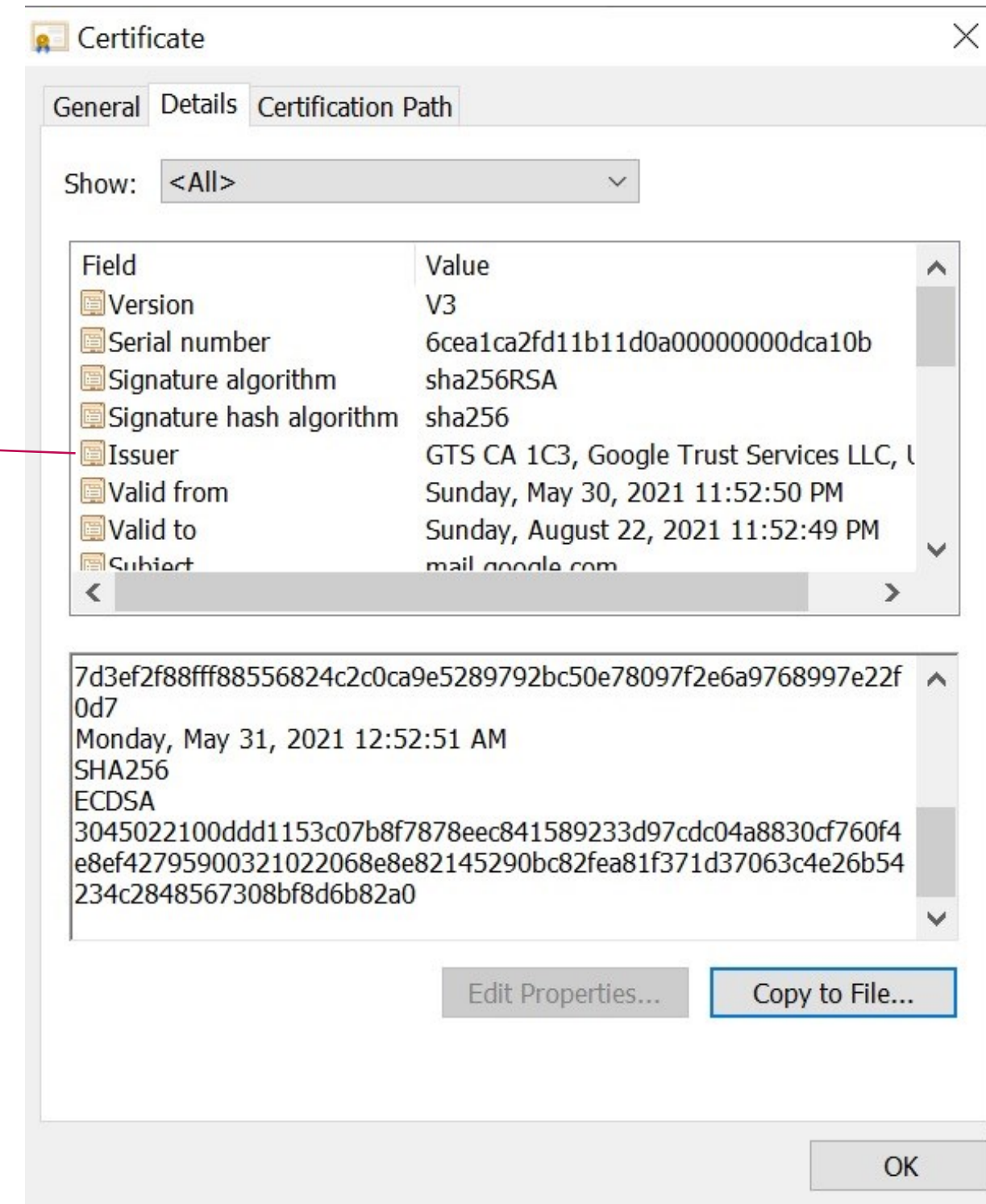
X.509 Components

Algorithm used by CA to sign certificate



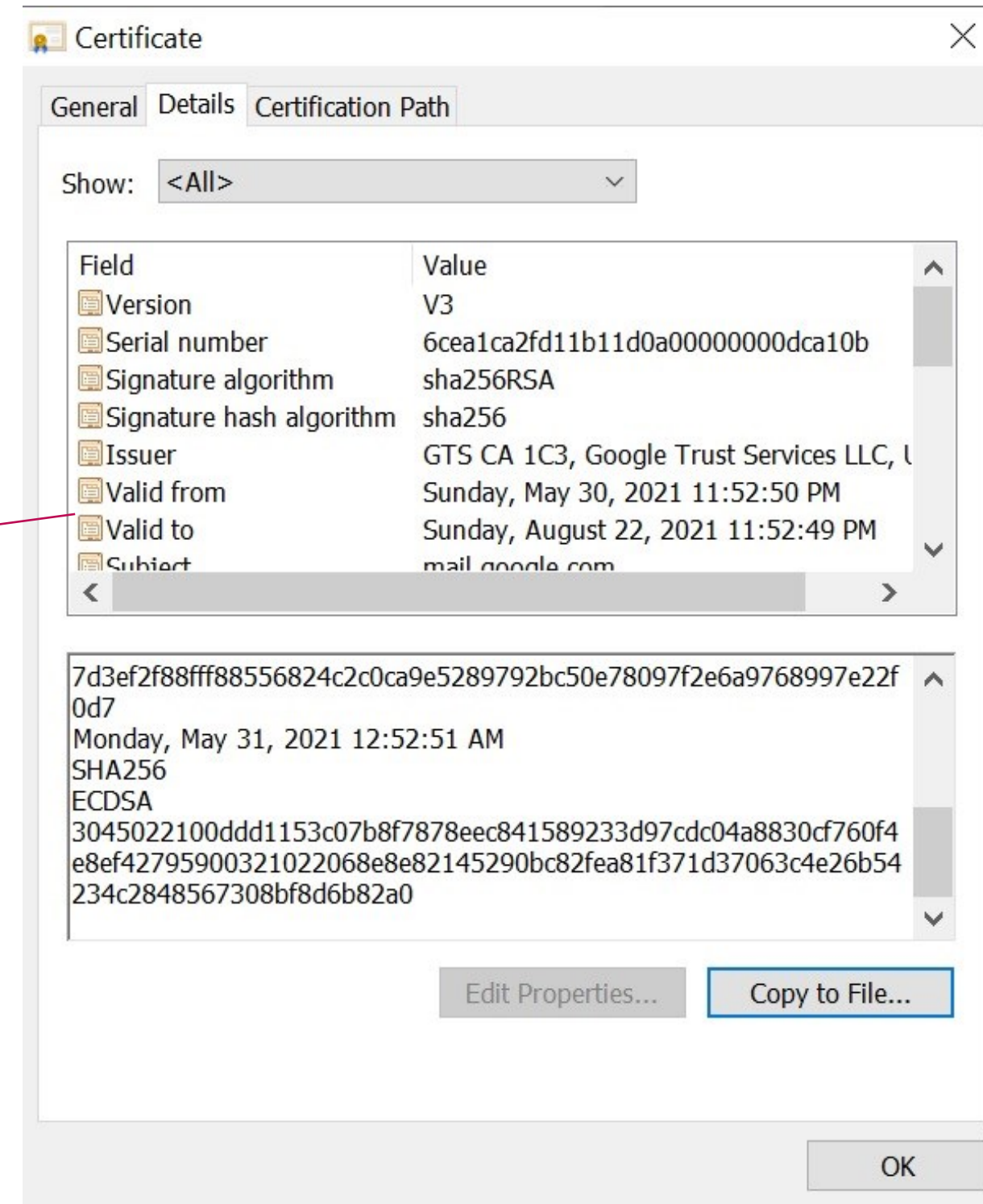
X.509 Components

CA that issues certificate



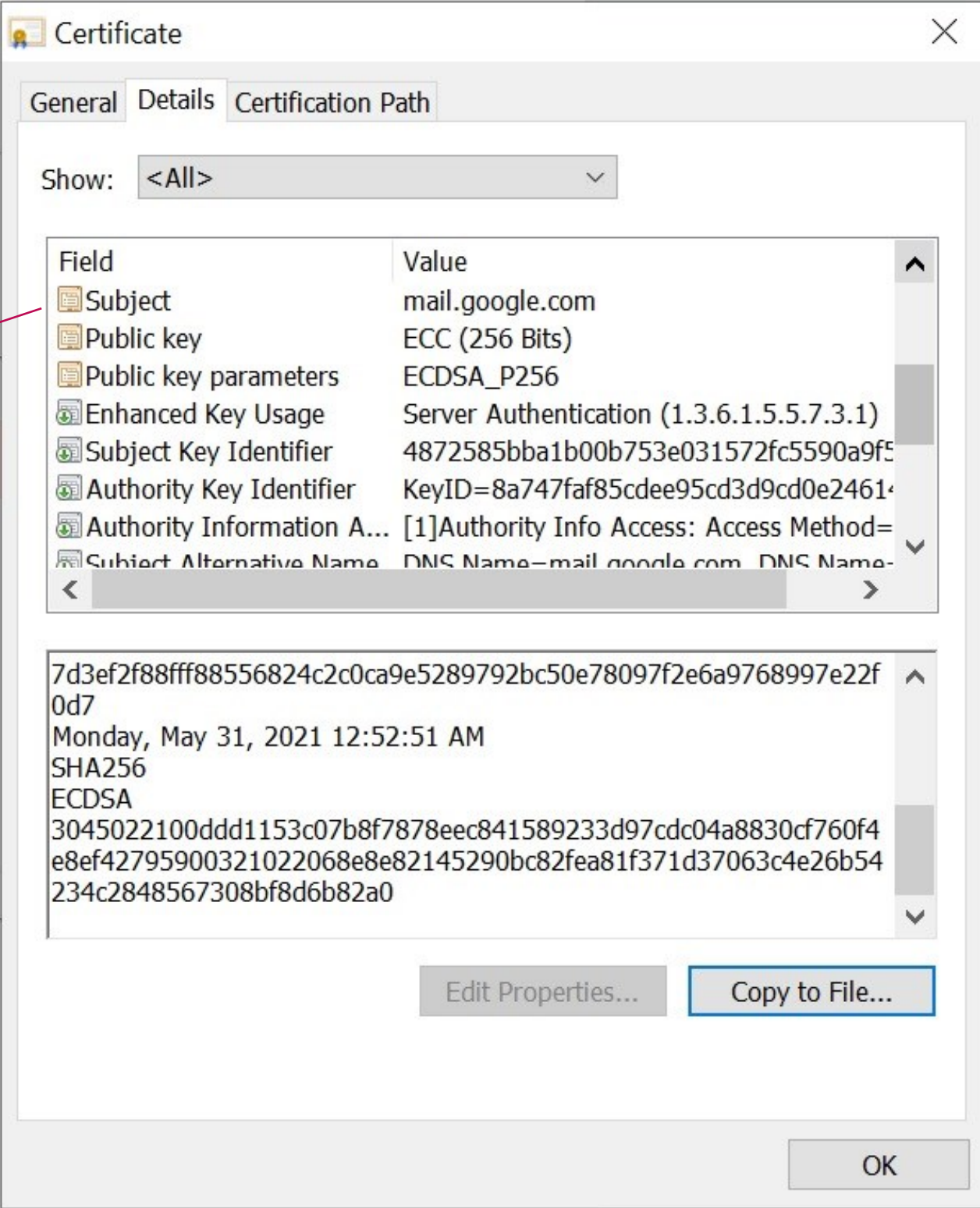
X.509 Components

Length of time certificate is valid



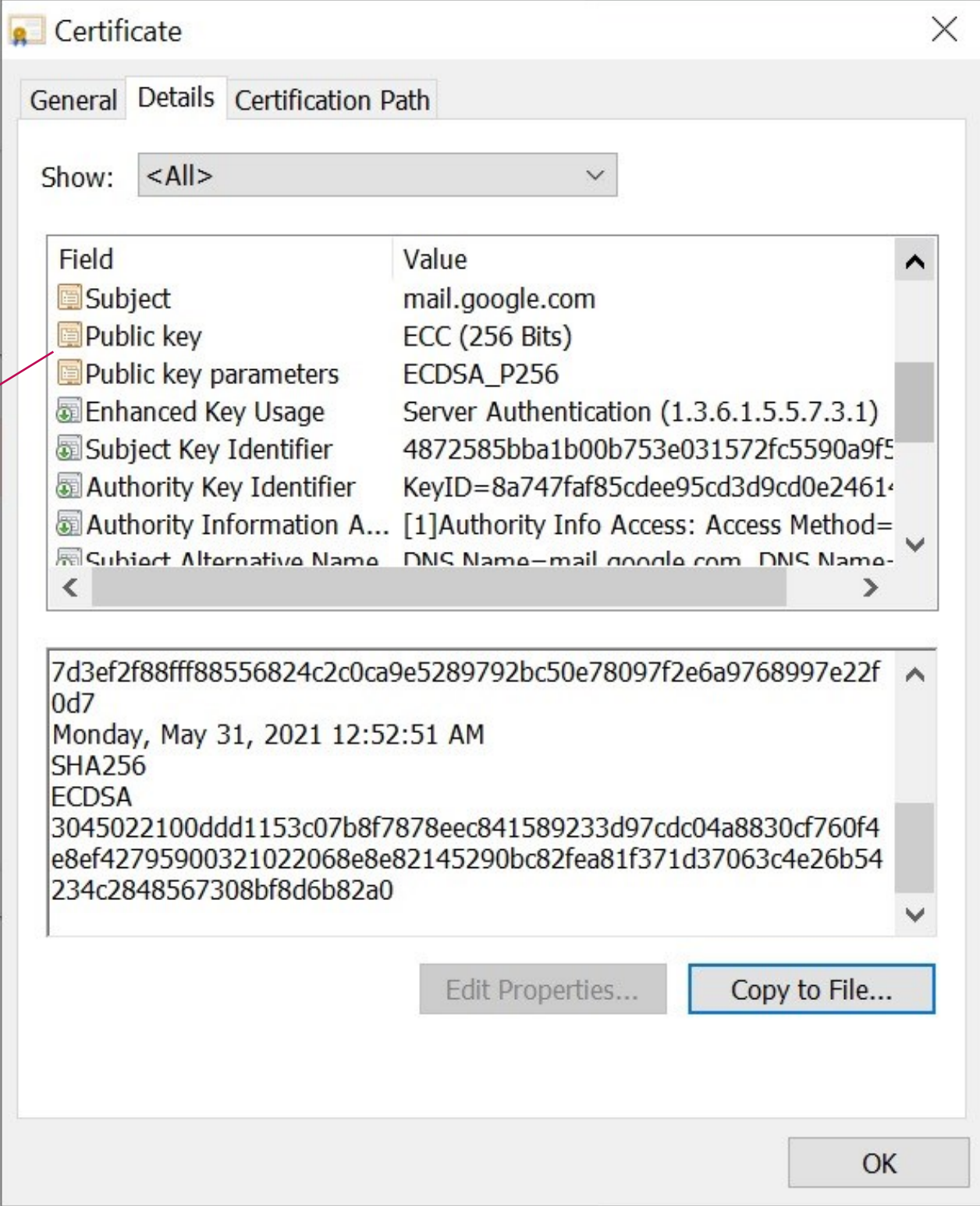
X.509 Components

Owner of public key

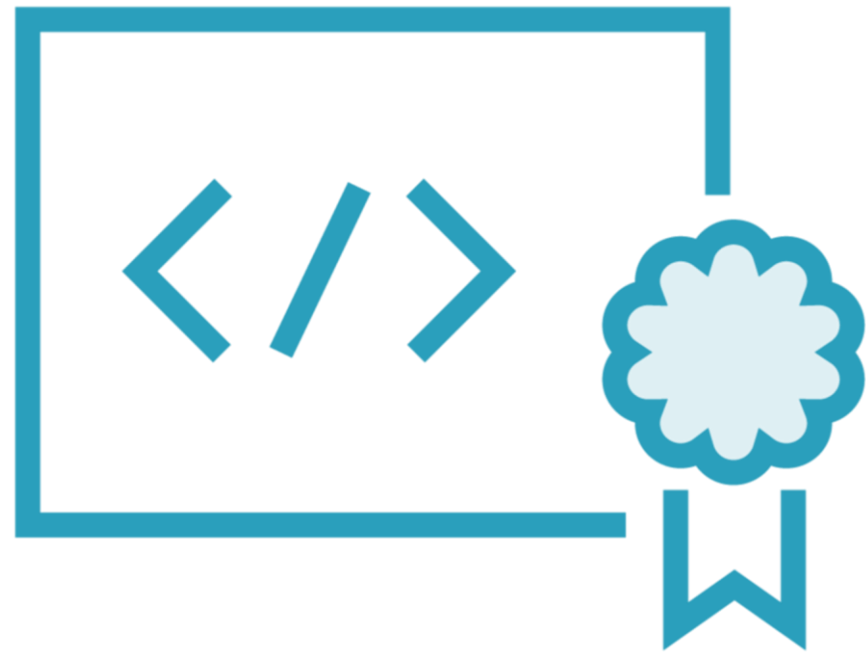


X.509 Components

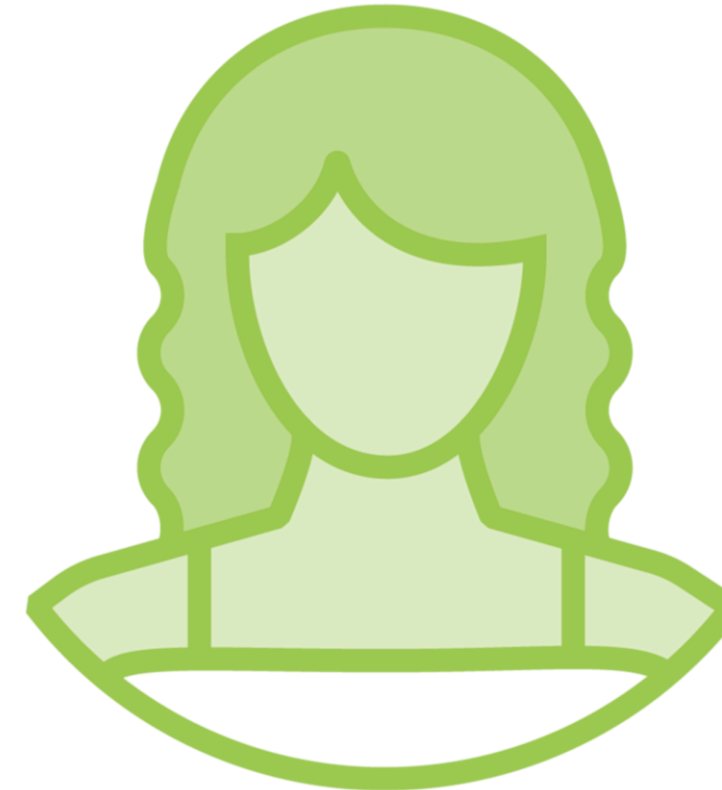
Public key data



X.509 Four Names and Two Roles



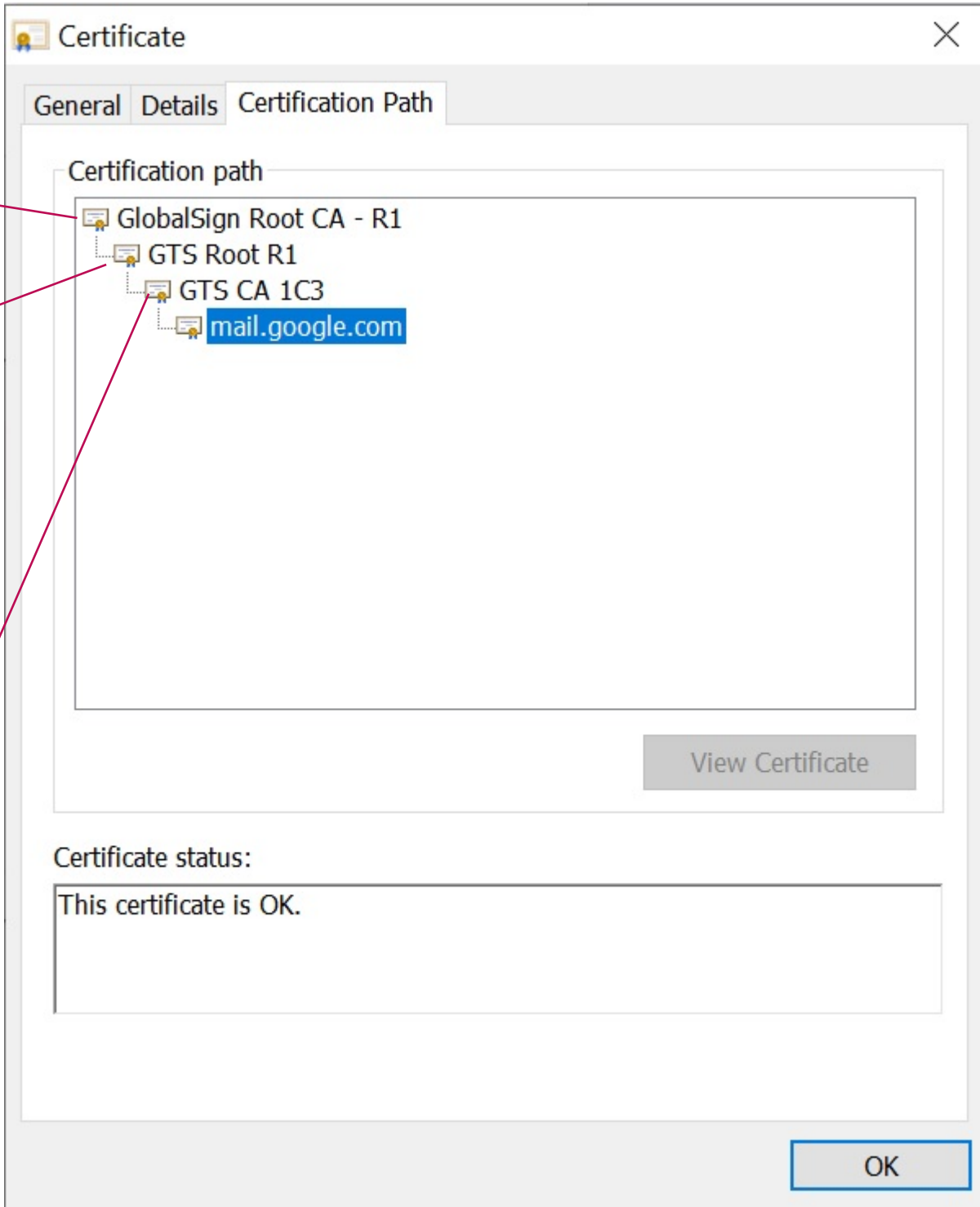
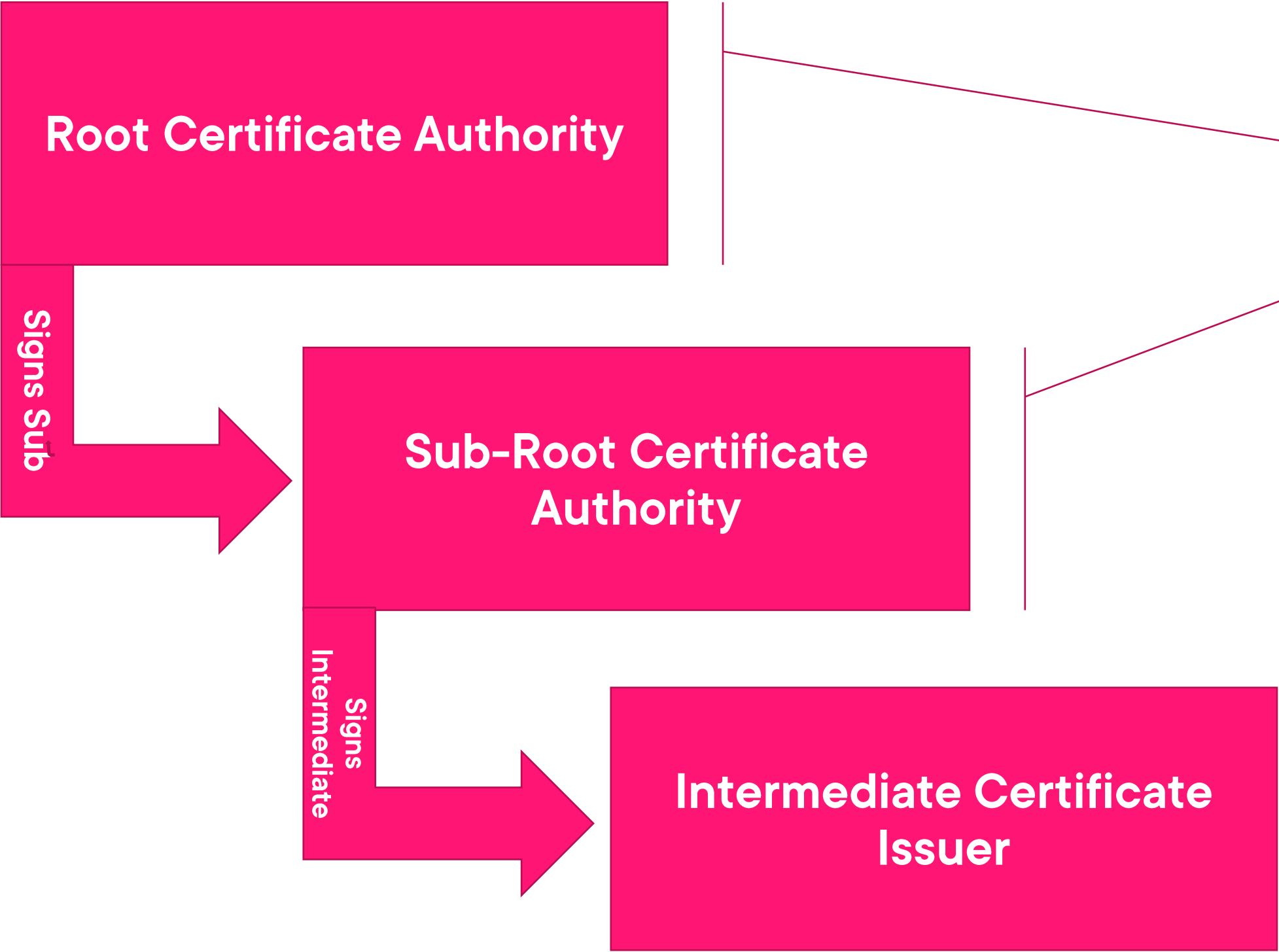
Certificate Authority / Issuer
Signer of digital certificate by
means of digital signature



Subject / Owner
Authenticated public key bound to
certificate of this entity



X.509 Hierarchical Chain of Trust



X.509 Local Trust Store

The screenshot shows the Windows Certificate Manager interface. The left pane displays the 'Trusted Root Certification Authorities' folder expanded to show a list of certificates. The right pane shows a table of certificates with columns for 'Issued To', 'Issued By', 'Expiration Date', and 'Intended Purposes'. A 'Certificate Information' dialog box is open, displaying details for a certificate issued by GlobalSign. The dialog includes a list of purposes, the issuer name, and the validity period.

Issued To	Issued By	Expiration Date	Intended Purposes
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authentication
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authentication
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authentication
Certum CA	Certum CA	6/11/2027	Client Authentication
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authentication

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data on disk to be encrypted
- Protects e-mail messages
- Allows secure communication on the Internet

Issued to: GlobalSign

Issued by: GlobalSign

Valid from: 3/18/2009 to 3/18/2029

Issuer Statement

OK



Single domain
Multi-domain
Wildcard certificates
Multi-domain wildcard

Types of X.509 certificates



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



Ciphertext



Bad actor



Known Plaintext Attack



Plaintext



Ciphertext



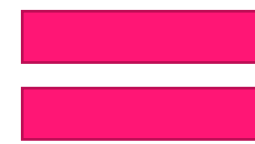
Bad actor



Known Plaintext Attack



Plaintext



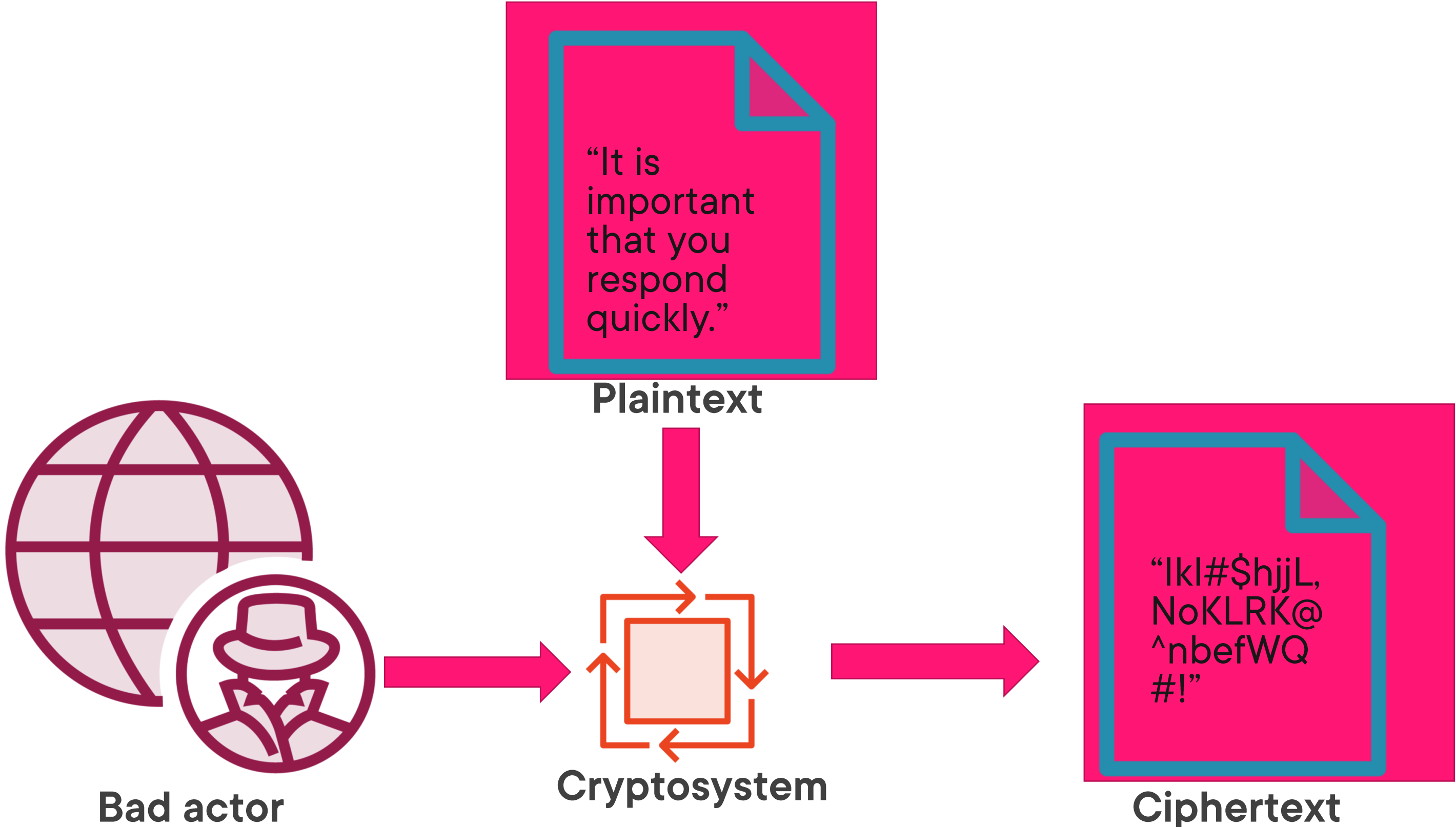
Ciphertext



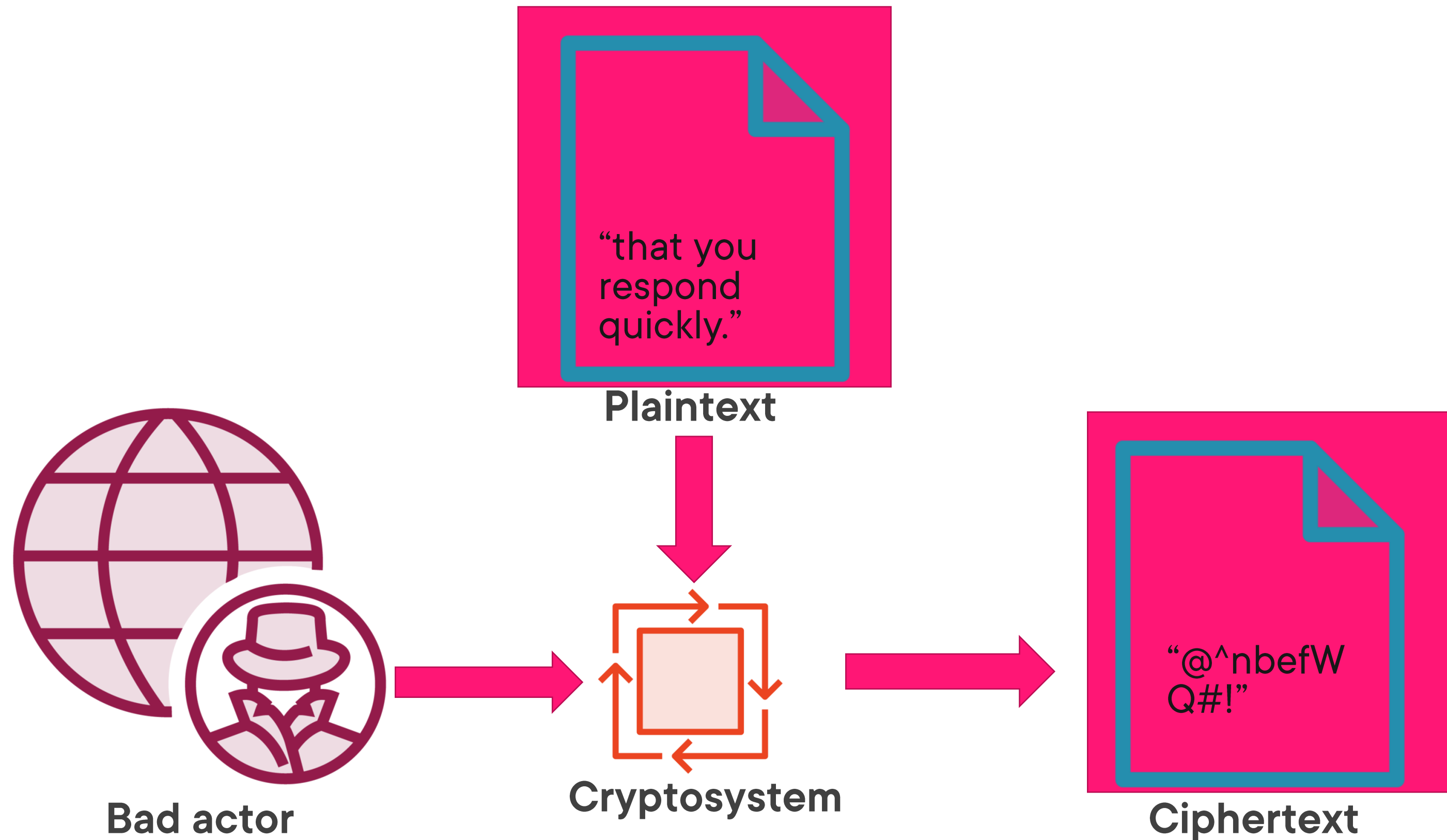
Bad actor



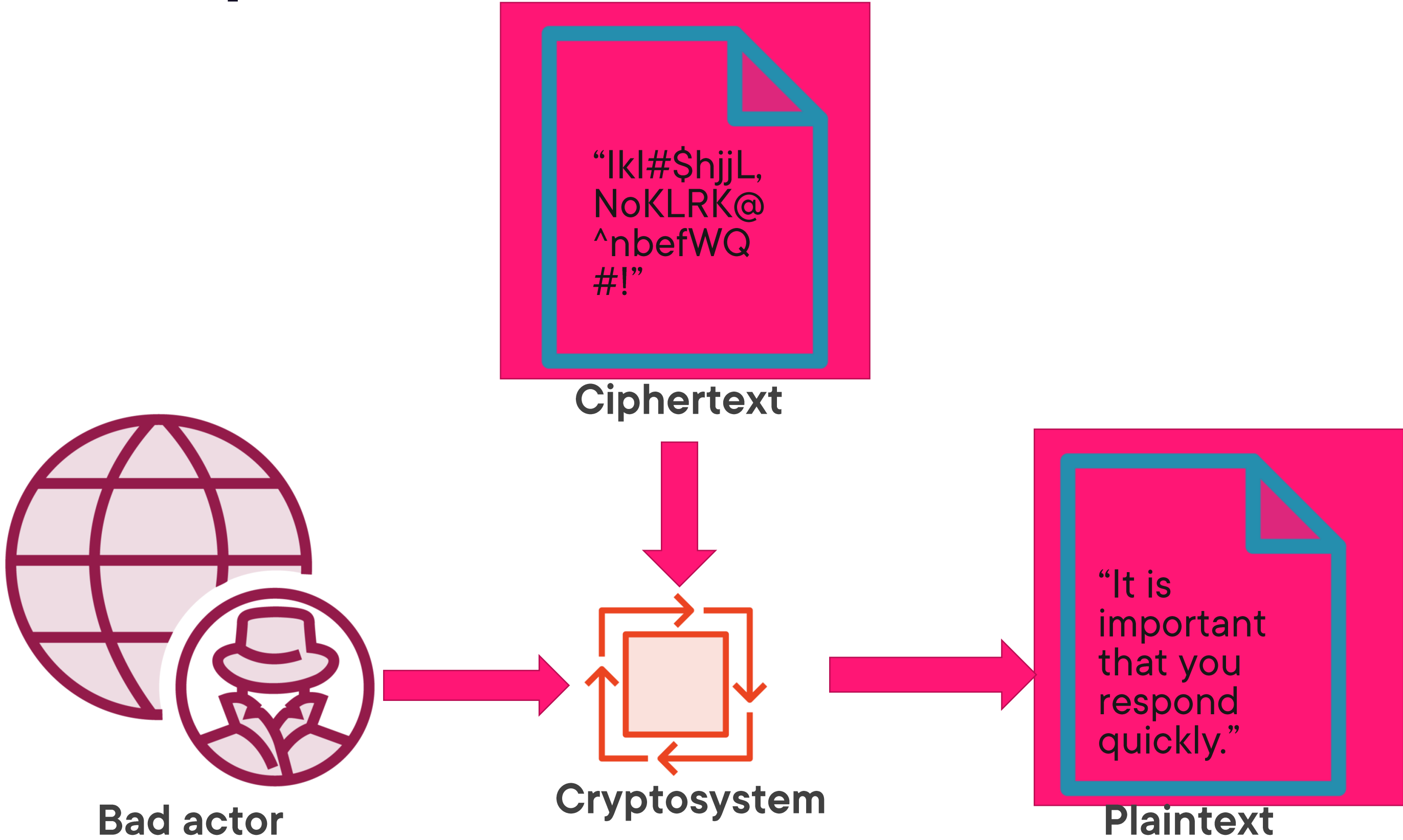
Chosen Plaintext Attack



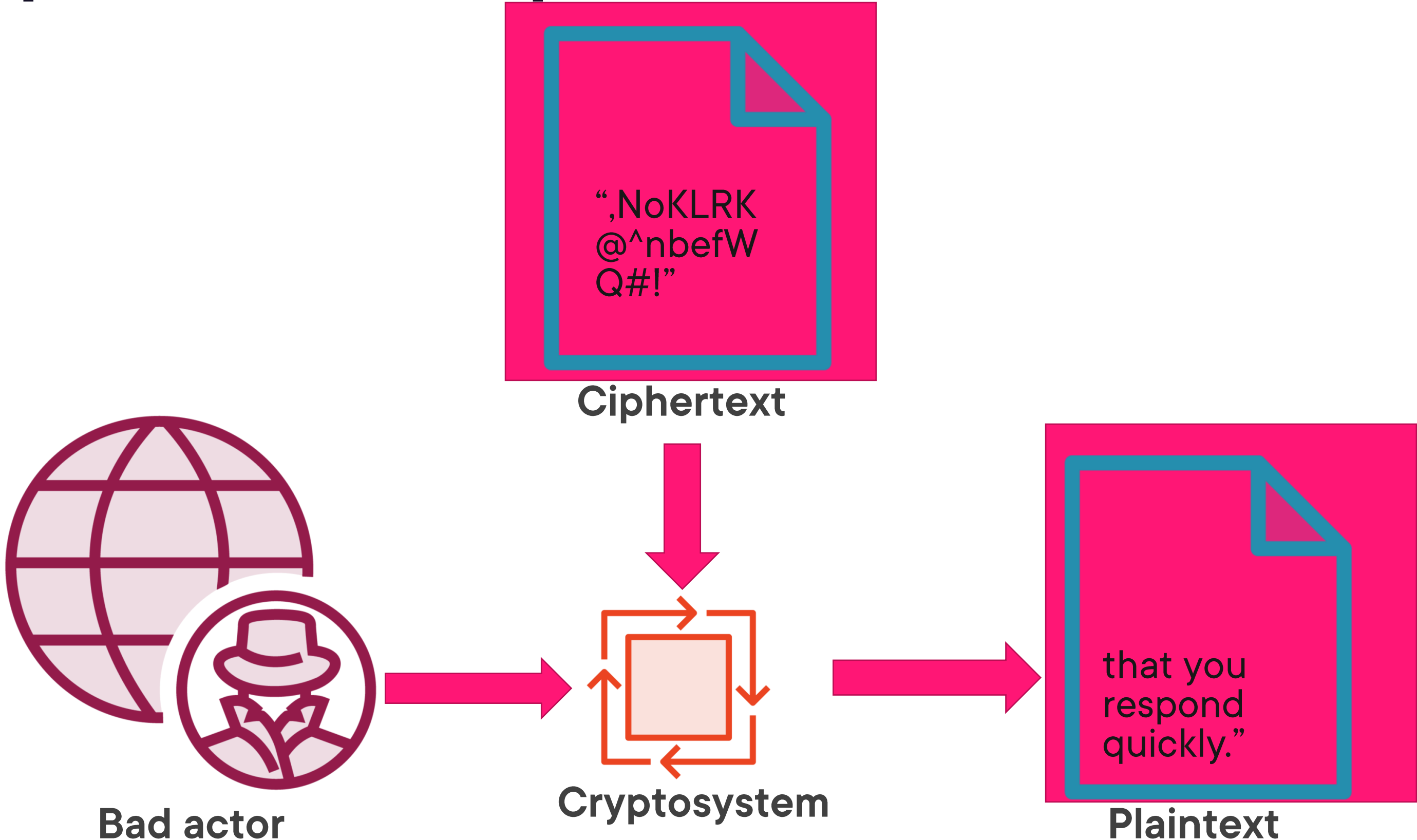
Adaptive Chosen Plaintext Attack



Chosen Ciphertext Attack



Adaptive Chosen Ciphertext Attack



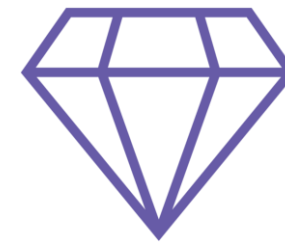
Key Management Principles



Key Management Provisions



Policy management protocols



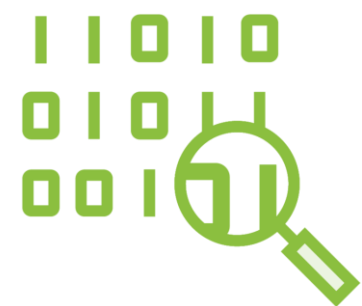
Crypto standards



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



Cryptographic Standard

Federal Information Processing Standard (FIPS) 140-3

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

NIST SP 800-175B

Post-Quantum Cryptography Standards

