CIT 270: SYSTEMS SECURITY I

CHAPTER 4: ADVANCED CRYPTOGRAPHY & PKI

BYU
IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

IMPLEMENTING CRYPTOGRAPHY

Key strength is made up of three primary characteristics:

- randomness (not predictable)
- length
- cryptoperiod (how long is it used)

Key Length	Key Space	Average Number of Attempts to Break
4	456,976	228,488
5	11,881,376	5,940,688
6	308,915,776	154,457,888
7	8,031,810,176	4,015,905,088
8	208,827,064,576	104,413,532,288

IMPLEMENTING CRYPTOGRAPHY

DARKNET DIARIES
EP 12: CRYPTO WARS

ALGORITHM SOUP
ALGORITHM… USED
TO BREAK... RSA KEYS

IMPLEMENTING CRYPTOGRAPHY

Electronic Code Book (ECB): a type of block cipher that splits the data into blocks and then encrypts each block separately; duplicates can occur.

Cipher Block Chaining (CBC): a block cipher where once encrypted the blocks are feed back into the encryption process; preceding block used on current.

Counter (CTR): sender and receiver use the same counter to encrypt each block of a message.

Galois/Counter (GCM): similar to CTR but adds an *additional authentication data* to the transmission; ensures the message was created by the sender.

IMPLEMENTING CRYPTOGRAPHY

Salt: a value that can be used to ensure a hash or key will not always result in the same digest; can be reused.

Nonce: a number used once is an input that must be unique within some specified scope.

Initialization Vector (IV): a nonce selected in a non-predictable way. An IV must be unpredictable or at least unique for each message encrypted with a given key.

DIGITAL CERTIFICATES

Digital Signatures have a weakness: they do not confirm the true identity of the sender only that the sender's private key was used to encrypt the signature.

Digital Certificates: used to associate a user's identity with a public key that has been digitally signed by a trusted third party.

IMPLEMENTING CRYPTOGRAPHY

Certificate Signing Request (CSR): a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Often a CSR contains the public key for which the certificate should be issued.

Intermediate Certificate Authority (ICA): subordinate entity that processes the CSR and verifies the authenticity of the user; pefromes functions on behalf of the CA.

Certificate Authority (CA): the root certificate authority is responsible for digitally signed certificates.

IMPLEMENTING CRYPTOGRAPHY

Offline CA: reduces the risk of certificate breach by keeping the server of certificates offline. Infrequently online only for specific tasks like issuance or re-issuance of certificates authorizing; removable storage can be used to update or issue intermediate CA's

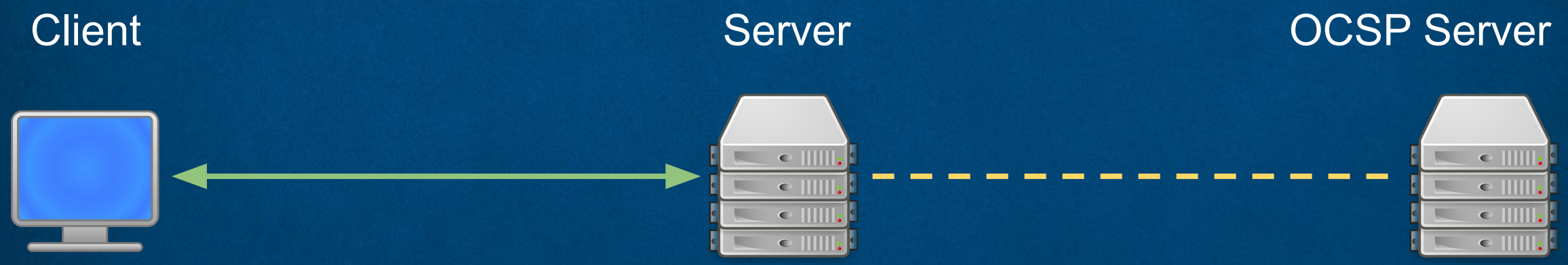
Online CA: usually intermediate CA's that can handle certificate authentication.

Certificate Revocation List (CRL): one method of checking to see if a certificate has been revoked using a list of serial numbers that have been revoked.

Online Certificate Status Protocol (OCSP): another method of checking a certificates status using a real-time lookup of a certificates status.

IMPLEMENTING CRYPTOGRAPHY

Stapling is a variation of OCSP where web servers periodically do their own certificate check and then include (staple) their OCSP response to clients (browsers) connecting to them so they can determine if the response is trustworthy.



Web browser opens a connection to the server over HTTPS. Server responds with a stapled response of its own OCSP query.

Server periodically performs an OCSP query on it's SSL certificate and saves the result.

IMPLEMENTING CRYPTOGRAPHY

Certificate Chaining links several certificates together to establish trust between all the certificates involved.

IMPLEMENTING CRYPTOGRAPHY

Key Exchange is the official name for the handshake web servers have with your web browser when you attempt to connect securely to them.

If all goes correctly with the handshake session keys are generated which can now be used to encrypt and decrypt information exchanged during the life of the session.

Don’t click *remember me on this device* when using public computers!

IMPLEMENTING CRYPTOGRAPHY

Key Exchange Process

Web Browser

Web Server

1. ClientHello. Cryptographic Information.

2. ServerHello. Algorithms Supported. Digital Certificate.

3. Verifies certificate and creates pre-master secret

3. ClientKeyExchange. Pre-master secret.

4. Creates master secret and session keys.

4. Creates master secret and session keys.

IMPLEMENTING CRYPTOGRAPHY

Domain Validation Digital Certificate: verifies the identity of the entity that has control over the domain name.

Extended Validation (EV) Certificate: requires more extensive verification of the legitimacy of the business; audit, officer signature, paperwork.

Wildcard Digital Certificate: validates a main domain name and all subdomains.

Subject Alternative Name (SAN): aka. *Unified Communications Certificate* (UCC) allows multiple servers to use the same certificate by allowing different values to be associated with the certificate.

IMPLEMENTING CRYPTOGRAPHY

Code Signing Digital Certificates: used by software developers to digitally sign a program to prove they software comes from their business.

Email Digital Certificates: allows users to digitally sign and encrypt email.

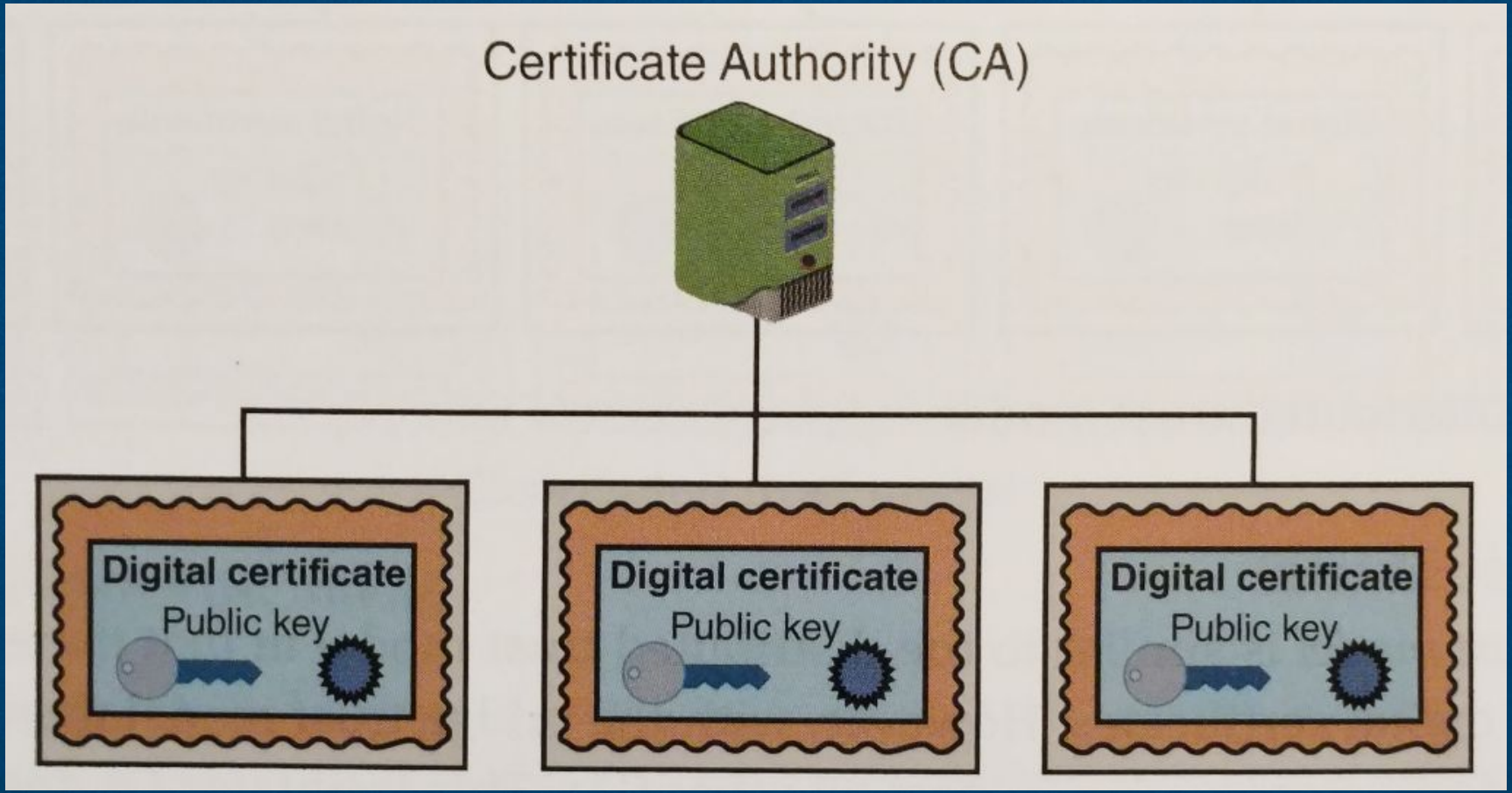
PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI): the underlying infrastructure for the management of public keys used in digital certificates; hardware, software, people, policies…

Trust Model: general term referring to the trust relationship between individuals and entities.

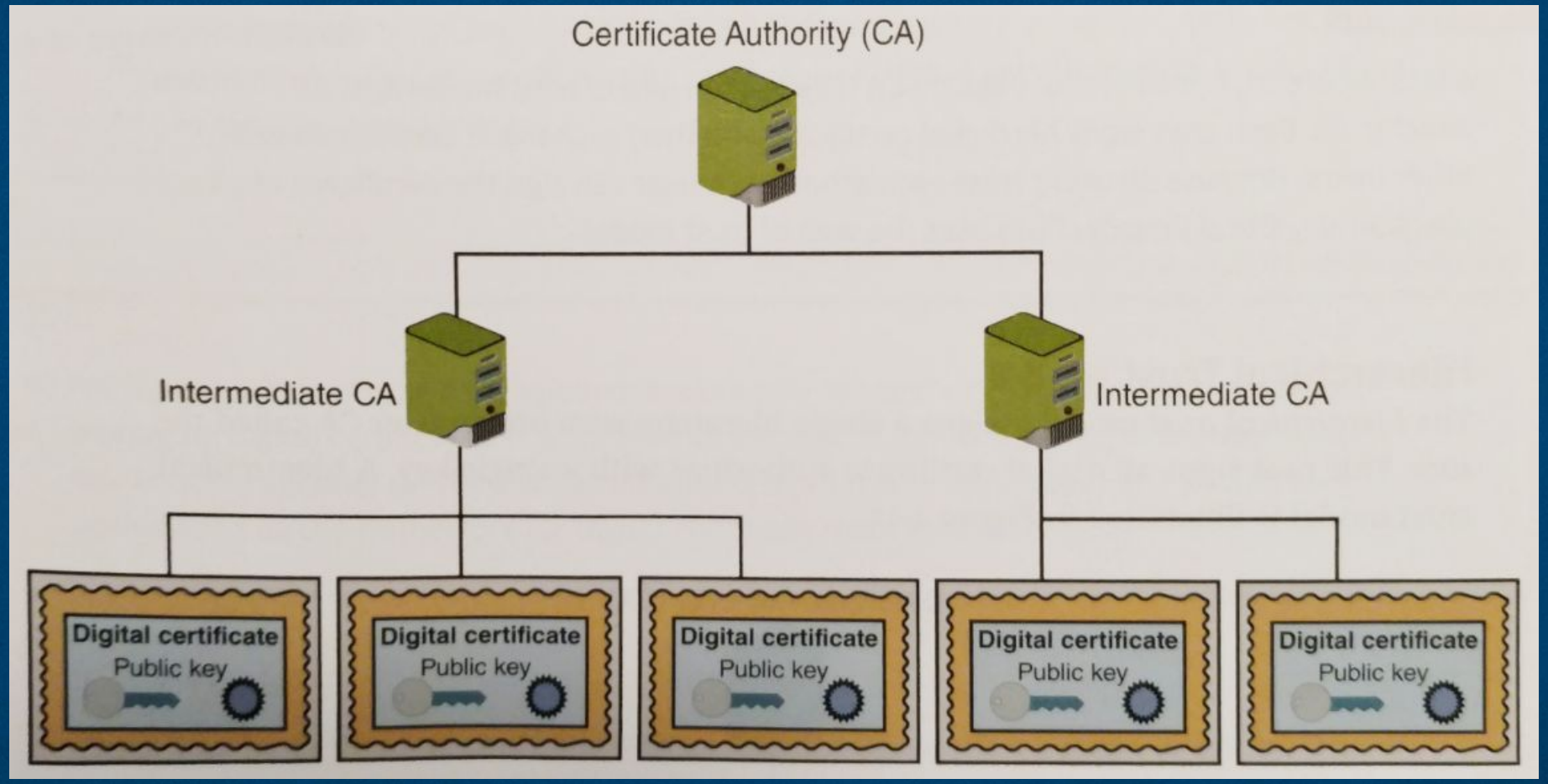
- Direct trust for example is where you know the person or entity personally.
- Third-party trust is when there is a common party you trust; courtroom.

PUBLIC KEY INFRASTRUCTURE



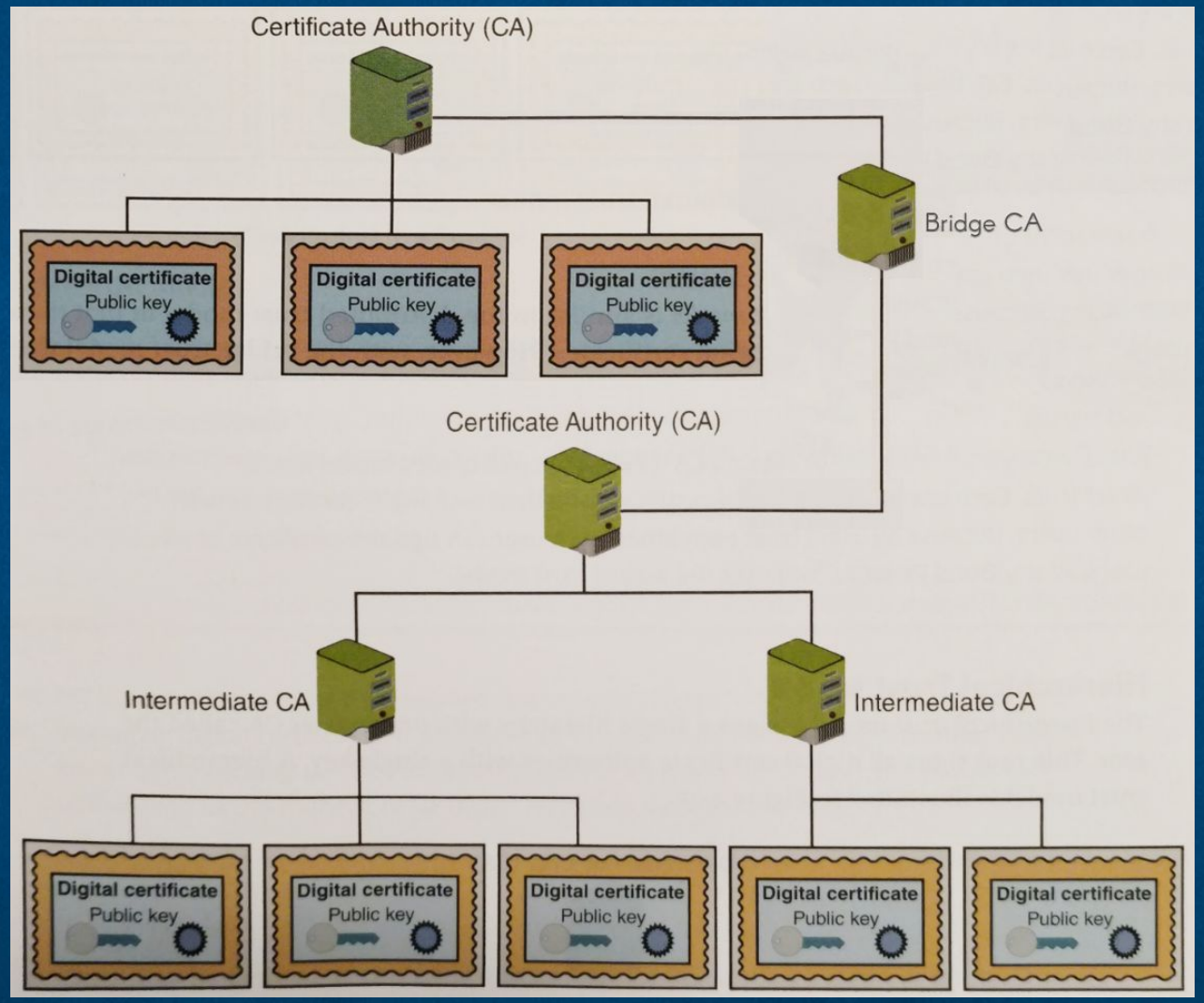
Hierarchical Trust Model

PUBLIC KEY INFRASTRUCTURE



Distributed Trust Model

PUBLIC KEY INFRASTRUCTURE



Bridged Trust Model

PUBLIC KEY INFRASTRUCTURE

Certain procedures help ensure keys are properly handled:

- Key Escrow: key managed by CA, private key split in half. 
- Expiration: keys expire after a set time.
- Renewal: expiration dates can be extended; convenient but vulnerable.
- Revocation: expiring a key early for a specific reason; terminated employee.
- Recovery: techniques to recover a lost or inaccessible key; M-of-N control.
- Suspension: a temporary revocation; employee leave.
- Destruction: a removal of all private and public keys along with the user's identification information from the CA; revocation and expirations do not destroy the CA record of you.

CRYPTOGRAPHIC TRANSPORT PROTOCOLS

Used for communications from web browsers and servers:

- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Hypertext Transport Protocol Secure (HTTPS)

Used for email communications:

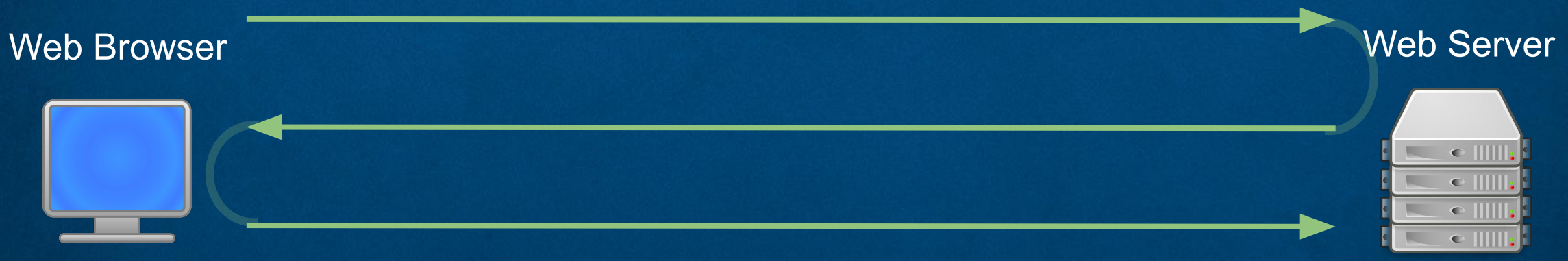
- Secure/ Multipurpose Internet Mail Extensions (S/MIME)

Used for Voice-over-IP (VoIP):

- Secure Real-time Transport Protocol (SRTP)

CRYPTOGRAPHIC TRANSPORT PROTOCOLS

Internet Protocol Security (IPsec) is the newest protocol and secures IP communications by encrypting and authenticating each IP packet between hosts or networks; can be transparent.



REFERENCES

Anti-mark [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Bridge Trust Model [Figure 4-14]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 169. Boston, MA: Cengage.

Certificate Chaining [Figure 4-5]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 159. Boston, MA: Cengage.

Distributed Trust Model [Figure 4-13]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 168. Boston, MA: Cengage.

File Server Icon [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Golden Key Icon [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Hierarchical Trust Model [Figure 4-12]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 167. Boston, MA: Cengage.

REFERENCES

Key Strength [Table 4-1]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 148. Boston, MA: Cengage.

Key Exchange [Figure 4-9]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 162. Boston, MA: Cengage.

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

Monitor Icon [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.