Lesson 6

Implementing Public Key Infrastructure

Topic 6A

Implement Certificates and Certificate Authorities

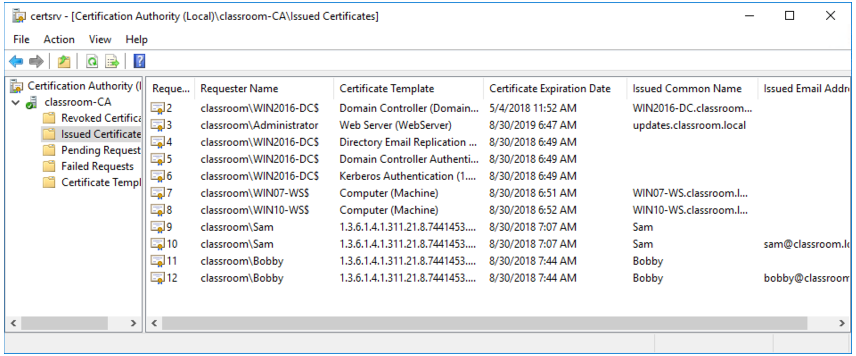
Syllabus Objectives Covered

- 3.9 Given a scenario, implement public key infrastructure

Public and Private Key Usage

- Public key cryptography
  - When you want others to send you confidential messages, you give them your public key to use to encrypt the message
  - When you want to authenticate yourself to others, you create a signature and sign it by encrypting the signature with your private key
- But how does someone trust the public key?
- Public key infrastructure (PKI) validates the identity of the owner of a public key
- Public key is wrapped in a digital certificate signed by a certificate authority (CA)
- Sender and recipient must both trust the CA

Certificate Authorities

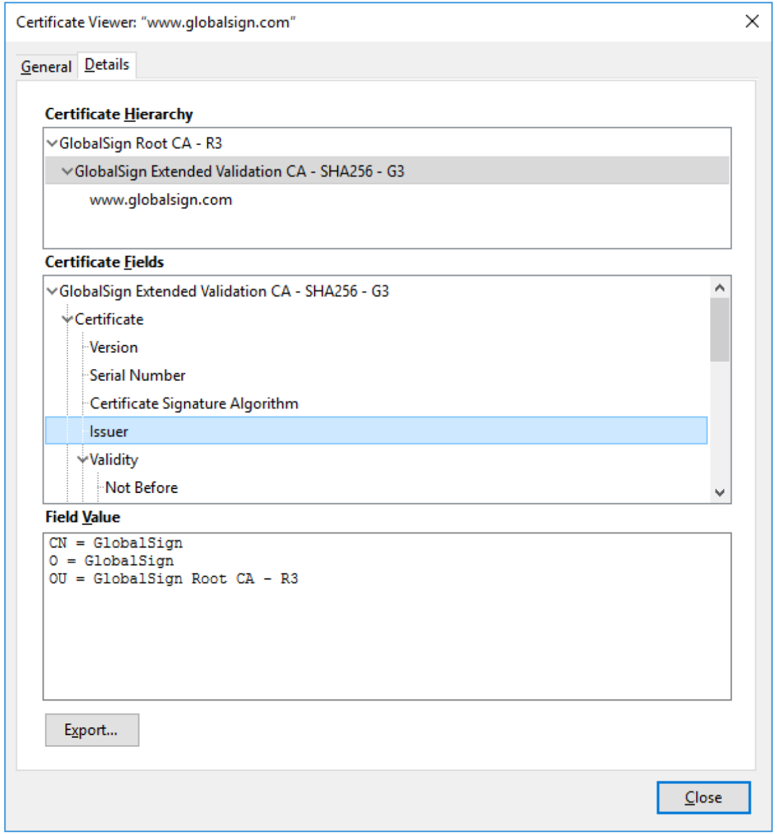


Reque...	Requester Name	Certificate Template	Certificate Expiration Date	Issued Common Name	Issued Email Addr
2	classroom\WIN2016-DC$	Domain Controller (Domain...	5/4/2018 11:52 AM	WIN2016-DC.classroom...	
3	classroom\Administrator	Web Server (WebServer)	8/30/2019 6:47 AM	updates.classroom.local	
4	classroom\WIN2016-DC$	Directory Email Replication ...	8/30/2018 6:49 AM		
5	classroom\WIN2016-DC$	Domain Controller Authenti...	8/30/2018 6:49 AM		
6	classroom\WIN2016-DC$	Kerberos Authentication (1....	8/30/2018 6:49 AM		
7	classroom\WIN07-WS$	Computer (Machine)	8/30/2018 6:51 AM	WIN07-WS.classroom.l...	
8	classroom\WIN10-WS$	Computer (Machine)	8/30/2018 6:52 AM	WIN10-WS.classroom.l...	
9	classroom\Sam	1.3.6.1.4.1.311.21.8.7441453....	8/30/2018 7:07 AM	Sam	
10	classroom\Sam	1.3.6.1.4.1.311.21.8.7441453....	8/30/2018 7:07 AM	Sam	sam@classroom.lo
11	classroom\Bobby	1.3.6.1.4.1.311.21.8.7441453....	8/30/2018 7:44 AM	Bobby	
12	classroom\Bobby	1.3.6.1.4.1.311.21.8.7441453....	8/30/2018 7:44 AM	Bobby	bobby@classroom

Screenshot used with permission from Microsoft.

- Private CAs versus third-party CAs
- Define services offered
- Ensure validity of certificates and users
- Establish trustworthy working procedures
- Manage servers and keys

PKI Trust Models and Certificate Chaining



Certificate Hierarchy

- GlobalSign Root CA - R3
  - GlobalSign Extended Validation CA - SHA256 - G3
    - www.globalsign.com

Certificate Fields

- GlobalSign Extended Validation CA - SHA256 - G3
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

Field Value

```
CN = GlobalSign
O = GlobalSign
OU = GlobalSign Root CA - R3
```

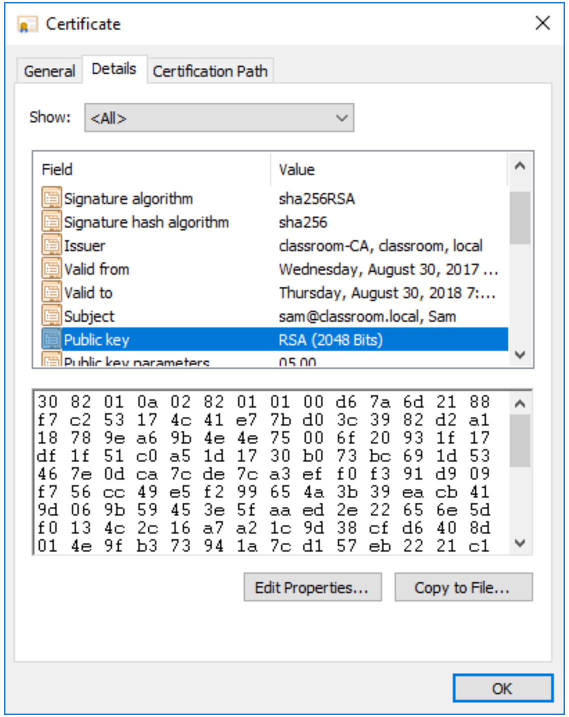
Screenshot used with permission from Microsoft.

- Single CA
- Hierarchical/chain of trust
  - Root CA
  - Intermediate CAs
  - Leaf certificates
- Online versus offline

Registration and CSRs

- Registration identification and authentication procedures
  - Private versus third-party CAs
- Certificate Signing Request (CSR)
  - Client generates key pair and sends public key to CA with CSR
  - CA performs subject identity checks
  - CA signs and issues certificate
- Registration authority (RA)

Digital Certificates



Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	classroom-CA, classroom, local
Valid from	Wednesday, August 30, 2017 ...
Valid to	Thursday, August 30, 2018 7:...
Subject	sam@classroom.local, Sam
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
30 82 01 0a 02 82 01 01 00 d6 7a 6d 21 88
f7 c2 53 17 4c 41 e7 7b d0 3c 39 82 d2 a1
18 78 9e a6 9b 4e 4e 75 00 6f 20 93 1f 17
df 1f 51 c0 a5 1d 17 30 b0 73 bc 69 1d 53
46 7e 0d ca 7c de 7c a3 ef f0 f3 91 d9 09
f7 56 cc 49 e5 f2 99 65 4a 3b 39 ea cb 41
9d 06 9b 59 45 3e 5f aa ed 2e 22 65 6e 5d
f0 13 4c 2c 16 a7 a2 1c 9d 38 cf d6 40 8d
01 4e 9f b3 73 94 1a 7c d1 57 eb 22 21 c1
```

Screenshot used with permission from Microsoft.

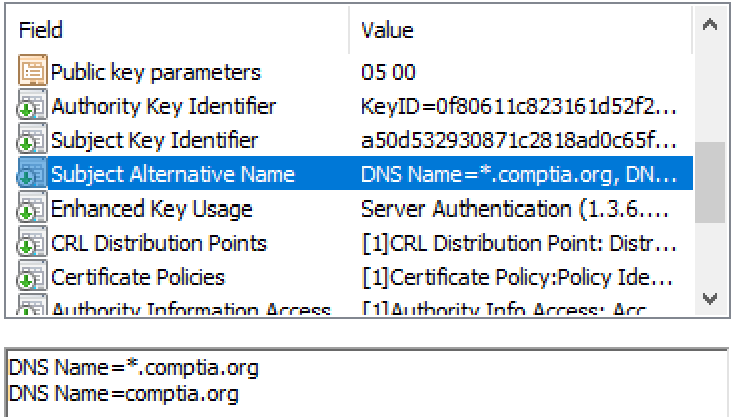
- Contains subject's public key
- Information identifying the subject plus usage and validity
- Digital certificate standards
  - X.509 Public Key Infrastructure (PKIX)
  - PKCS (Public Key Cryptography Standards)

Certificate Attributes

Field	Usage
Serial Number	A number uniquely identifying the certificate within the domain of its CA.
Signature Algorithm	The algorithm used by the CA to sign the certificate.
Issuer	The name of the CA.
Valid From/To	Date and time during which the certificate is valid.
Subject	The name of the certificate holder, expressed as a distinguished name (DN). Within this, the Common Name (CN) part should usually match either the fully qualified domain name (FQDN) of the server or a user email address.
Public Key	Public key and algorithm used by the certificate holder.
Extensions	V3 certificates can be defined with extended attributes, such as friendly subject or issuer names, contact email addresses, and intended key usage.
Subject Alternative Name (SAN)	This extension field is the preferred mechanism to identify the DNS name or names by which a host is identified.

Subject Name Attributes

- Common Name (CN)
  - Legacy method of recording FQDN
  - Deprecated by standards
  - BUT still used in many implementations
- Subject Alternative Name (SAN)
  - Structured identifiers
  - List multiple host/subdomains
  - Use wildcard subdomain



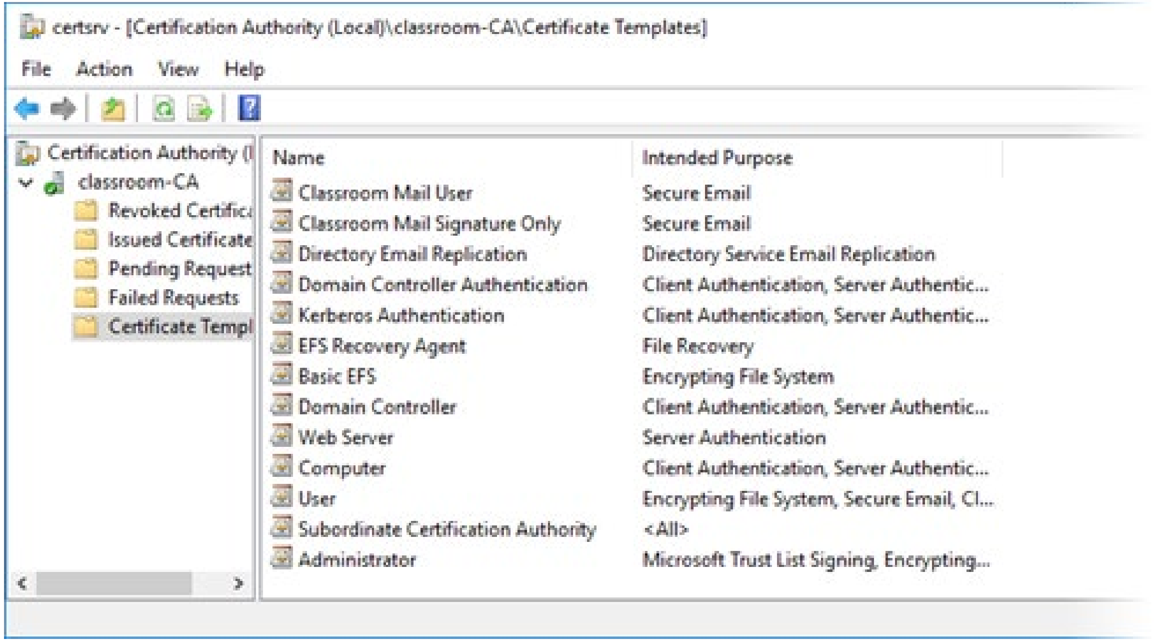
Field	Value
Public key parameters	05 00
Authority Key Identifier	KeyID=0f80611c823161d52f2...
Subject Key Identifier	a50d532930871c2818ad0c65f...
Subject Alternative Name	DNS Name=*.comptia.org, DN...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc

DNS Name=*.comptia.org
DNS Name=comptia.org

Screenshot used with permission from Microsoft.

Types of Certificate

- Certificate policies and templates
- Key usage
- Extended Key Usage/Enhanced Key Usage
- Critical or non-critical



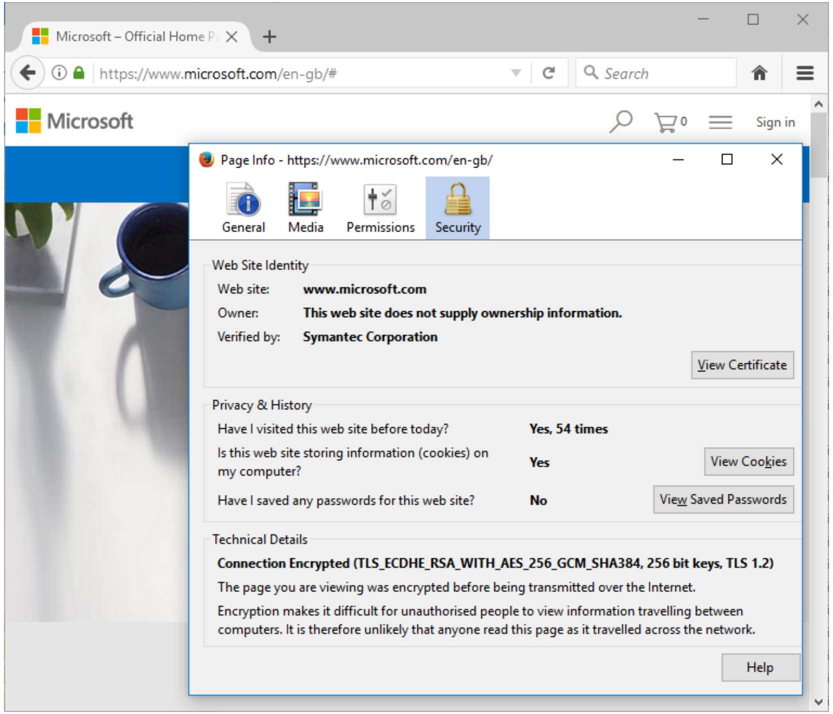
Name	Intended Purpose
Classroom Mail User	Secure Email
Classroom Mail Signature Only	Secure Email
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Screenshot used with permission from Microsoft.

Web Server Certificate Types

- Domain Validation (DV)
  - More rigorous identity checks
- Extended Validation (EV)
  - Even more rigorous identity checks

Screenshot used with permission from Microsoft.



Web Site Identity

Web site: **www.microsoft.com**

Owner: **This web site does not supply ownership information.**

Verified by: **Symantec Corporation**

Privacy & History

Have I visited this web site before today?	**Yes, 54 times**
Is this web site storing information (cookies) on my computer?	**Yes**
Have I saved any passwords for this web site?	**No**

Technical Details

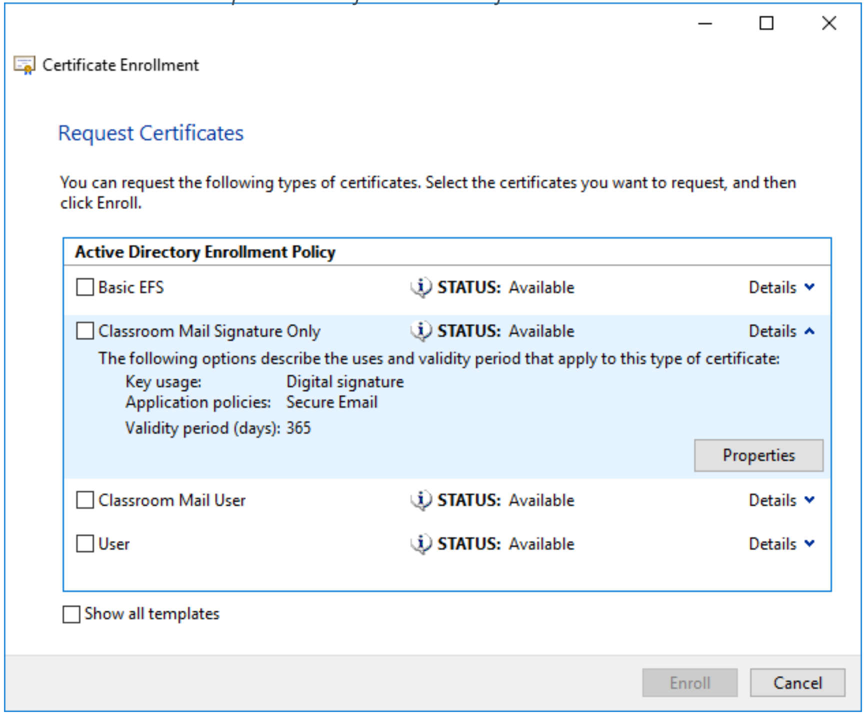
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

Other Certificate Types

Screenshot used with permission from Microsoft.



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Basic EFS **STATUS:** Available Details

□ Classroom Mail Signature Only **STATUS:** Available Details

The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Application policies: Secure Email
Validity period (days): 365

□ Classroom Mail User **STATUS:** Available Details

□ User **STATUS:** Available Details

□ Show all templates

- Machine/computer
  - Servers and network appliances
  - Identify by FQDN
- Email/user certificate
  - Can be various types (email, encryption, smart card logon, and so on)
  - Identify by email address
- Code signing
  - Validate publisher name
- Root certificate
  - Self-signed certificate for the CA
- Self-signed certificate
  - Must be manually trusted

Topic 6B

Implement PKI Management

Syllabus Objectives Covered

- 3.9 Given a scenario, implement public key infrastructure
- 4.1 Given a scenario, use the appropriate tool to assess organizational security (OpenSSL only)

Certificate and Key Management

- Key life cycle
  - Key generation
  - Certificate generation
  - Storage
  - Revocation
  - Expiration and renewal
- Vulnerabilities from improper management

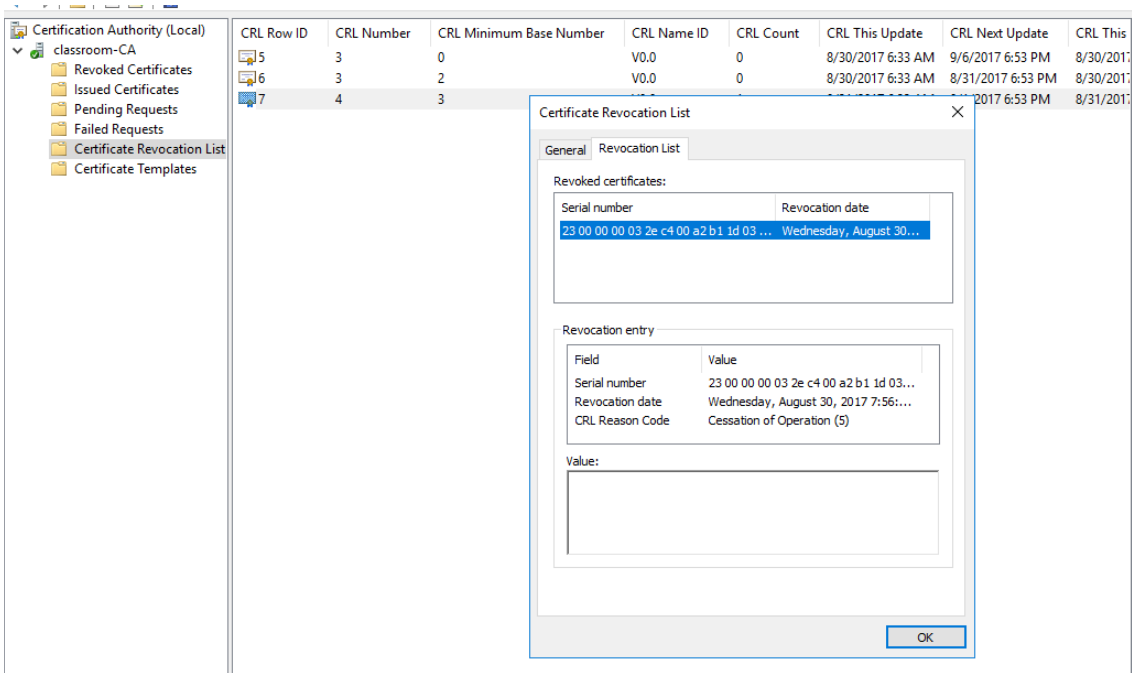
Key Recovery and Escrow

- M-of-N control for critical keys (root servers)
- Keys can be backed up to protect against data loss
  - Anyone with access to backup keys could impersonate the true key holder
  - Key recovery processes can be protected by M of N control
- Escrow backup
  - Placing archived keys with a trusted third party

Certificate Expiration

- Certificate duration
- Certificate renewal
  - Use existing key pair
  - Re-key with newly generated key pair
- Expiration
  - Public key will no longer be accepted
  - Archiving versus destroying key material
  - Secure erasing methods

Certificate Revocation Lists



- Certification Authority (Local)
  - classroom-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Revocation List
    - Certificate Templates

CRL Row ID	CRL Number	CRL Minimum Base Number	CRL Name ID	CRL Count	CRL This Update	CRL Next Update	CRL This
5	3	0	V0.0	0	8/30/2017 6:33 AM	9/6/2017 6:53 PM	8/30/201
6	3	2	V0.0	0	8/30/2017 6:33 AM	8/31/2017 6:53 PM	8/30/201
7	4	3				2017 6:53 PM	8/31/201

Certificate Revocation List

General | Revocation List

Revoked certificates:

Serial number	Revocation date
23 00 00 00 03 2e c4 00 a2 b1 1d 03 ...	Wednesday, August 30...

Revocation entry

Field	Value
Serial number	23 00 00 00 03 2e c4 00 a2 b1 1d 03...
Revocation date	Wednesday, August 30, 2017 7:56:...
CRL Reason Code	Cessation of Operation (5)

Value:

Screenshot used with permission from Microsoft.

- Revocation versus suspension
- Reason codes
- Certificate Revocation List (CRL)
  - List of revoked and suspended certificates
  - Browser CRL checking

Online Certificate Status Protocol Responders

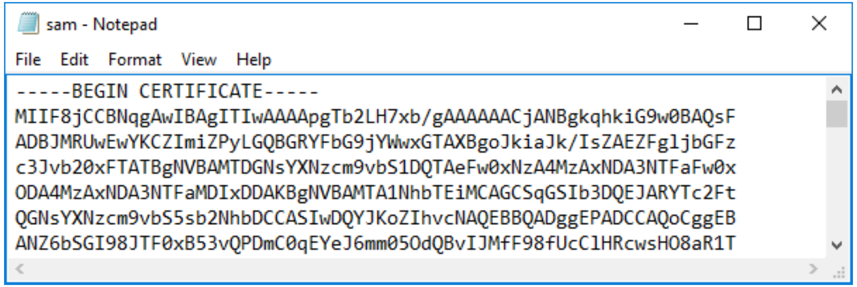
- Online Certificate Status Protocol (OCSP)
  - OCSP responder
  - Provide real-time status information (though some rely on CRLs)
  - Client queries single certificate per transaction
- OCSP stapling
  - Clients might need to make lots of certificate queries for a chain of trust
  - Queries can be used to track clients
  - Stapling proxies the OCSP response

Certificate Pinning

- Defend against MitM attacks on chain of trust
- Web server references authorized public key(s) in HTTP header
    - HTTP Public Key Pinning (HPKP)
    - Certificate Transparency framework

Certificate Formats

- Distinguished Encoding Rules (DER)
  - Binary format
- Privacy-enhanced Electronic Mail (PEM)
  - Represent binary as ASCII using Base64 encoding
- .CER and .CRT file formats may be either binary or ASCII
- Personal information exchange
  - Export a private key (binary and password-protected)
  - .PFX or .P12 (PKCS #12)
- Export a certificate chain
  - .P7B (PKCS #7)



```
-----BEGIN CERTIFICATE-----
MIIF8jCCBNqgAwIBAgITIwAAAApgTb2LH7xb/gAAAAAACjANBgkqhkiG9w0BAQsF
ADBJMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFgljbGFz
c3Jvb20xFTATBgNVBAMTDGNsYXNzcm9vbS1DQTAeFw0xNzA4MzAxNDA3NTFaFw0x
ODA4MzAxNDA3NTFaMDIxDDAKBgNVBAMTA1NhbTEiMCAGCSqGSIb3DQEJARYTc2Ft
QGNsYXNzcm9vbS5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANZ6bSGI98JTF0xB53vQPDmC0qEYeJ6mm05OdQBvIJMfF98fUcClHRcwsHO8aR1T
```

Screenshot used with permission from Microsoft.

OpenSSL

- Windows Certificate Services and certutil /PowerShell
- OpenSSL
  - Key pair generation and CA root certificate
  - Certificate requests
  - Viewing and verifying certificates
  - Converting certificate formats

Certificate Issues

- Troubleshoot rejection of certificates by servers and clients
  - Existing certificate—check expiry and status
  - New certificate
    - Check key usage settings and requirements
    - Check subject name
    - Check chain of trust/root certificates
  - Verify time and date settings
- Audit certificate and PKI infrastructure

Lesson 6

Summary