Components Of Digital Certificates

Copyright © www.ine.com

https://t.me/learningnets

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Copyright © www.ine.com

https://t.me/learningnets

Topic Overview

- Common components of Digital Certificates

Copyright © www.ine.com

https://t.me/learningnets

Components Of Digital Certificates

- The content of a certificate varies depending on its prescribed use
- Most certificates contain;
  - X.509 version number
  - Certificate serial number
  - Cryptographic algorithm used for the signature
  - CA's digital signature
  - Issuing CA
  - Validity dates
  - Server name
  - Server public key
  - Key usage
  - Certificate policies
  - Revocation information.

RFC 5280

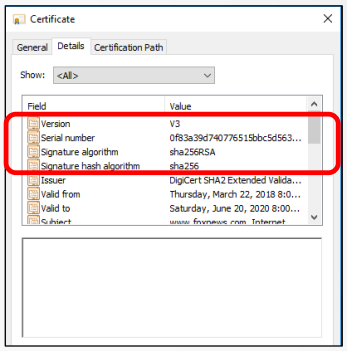
Copyright © www.ine.com

There are many more fields you'll probably see in a Certificate. This video is not meant to comprehensively cover them all.

https://t.me/learningnets

Components Of Digital Certificates

- Version: The most widely accepted format for certificates is defined by the ITU-T X.509 standard. Current standard has been set at version-3 since 1995.



- Serial Number: Unique identifier for each Certificate, issued by CA.
- Signature algorithm: Concatenation of two values:
  - Algorithm used to create the Hash Digest of the Certificate (SHA256) and…
  - Public Key Encryption Algorithm used to encrypt the Hash using Private Key of CA (RSA)
- Signature Hash Algorithm: Restatement of the algorithm used to create the Hash Digest.

Copyright © www.ine.com

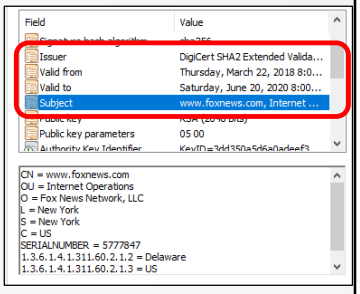
Serial number must fit within 20-bytes. Only unique to the CA…not necessarily globally unique.

-

https://t.me/learningnets

Components Of Digital Certificates

- Issuer: Provides a distinguished name for the CA that issued the certificate.
- Valid from: Date and time that Certificate first became valid.
- Valid to: Date and time that Certificate expires.
  - Most Certificates are issued for either two (2) or three (3) years.



- Subject: Provides the name of the computer, user, network device, or service that the CA issues the certificate to.

Copyright © www.ine.com

Issuer and Subject: commonly represented by using an X.500 or LDAP format

-

It would appear that CA's have quite a bit of leeway as to what they place into the "Subject" field.

-

If this Cert is for a website, then the DNS name of the site must be in the "subject" field.

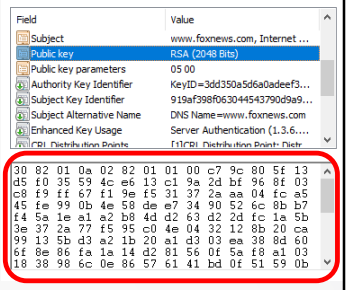
-

Multi-Domain (SAN) Certificate: Sometimes the "Subject" field doesn't seem to match up at all to the website you just visited, and yet the Certificate is accepted by the web browser. Why is this? This is because of an optional extension to Certs called the "Subject Alternative Name" field. More on this topic in the next slide.

https://t.me/learningnets

Components Of Digital Certificates

- Public Key: Public Key of the owner of the Certificate.
- Public Key Parameters: For Certificates using RSA encryption, this field must be “null”. 0500 represents “null”.
- Subject Alternative Name: allows additional identities to be bound to the subject of the certificate.



- Enhanced Key Usage: Indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes already indicated in the key usage extension.

Copyright © www.ine.com

Sub Alt Name: Typically you’ll find the DNS Name of the website in here which displays the FQDN (Fully-Qualified Domain Name) of the site. Can also include email addresses, IP addresses and URIs (Universal Resource Indicators).

-

There are some types of Certificates (such as “Shared TLS Certificates” and Multi-Domain (SAN) Certificates) that (at a reduced cost to the purchaser) allow multiple companies to share a single Certificate. This happens when multiple companies all have their websites hosted by a common Content Provider. View the Certificate from “bankrate.com” as an example.

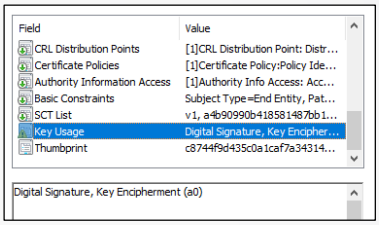
-

Enhanced Key Usage: In the next slide you see the field, “Key Usage”. That field is only 9-bits long, each bit indicating a flag. If someone wanted additional usages (or restrictions) of their public key beyond those 9-bits…they would utilize this “enhanced” field.

https://t.me/learningnets

Components Of Digital Certificates

- CRL Distribution Points: Pointer to a time-stamped list (signed by a CA) identifying revoked certificates
- Key Usage: Defines the purpose of the public key contained in a certificate. By default “Digital Signature” and “Key Encipherment” are set for Internet Certificates.
- Thumbprint: Contains the encrypted Digest (Hash) of the Certificate. This is the stamp of authenticity provided by the Issuer (CA).



Copyright © www.ine.com

CRL: Although a cert is expected to be valid during it’s stated lifetime, there can be circumstances in which it needs to be revoked (such as compromise of its Private Key).

Reinforce: see RFC 5280 for more details on all of the fields within a Certificate.

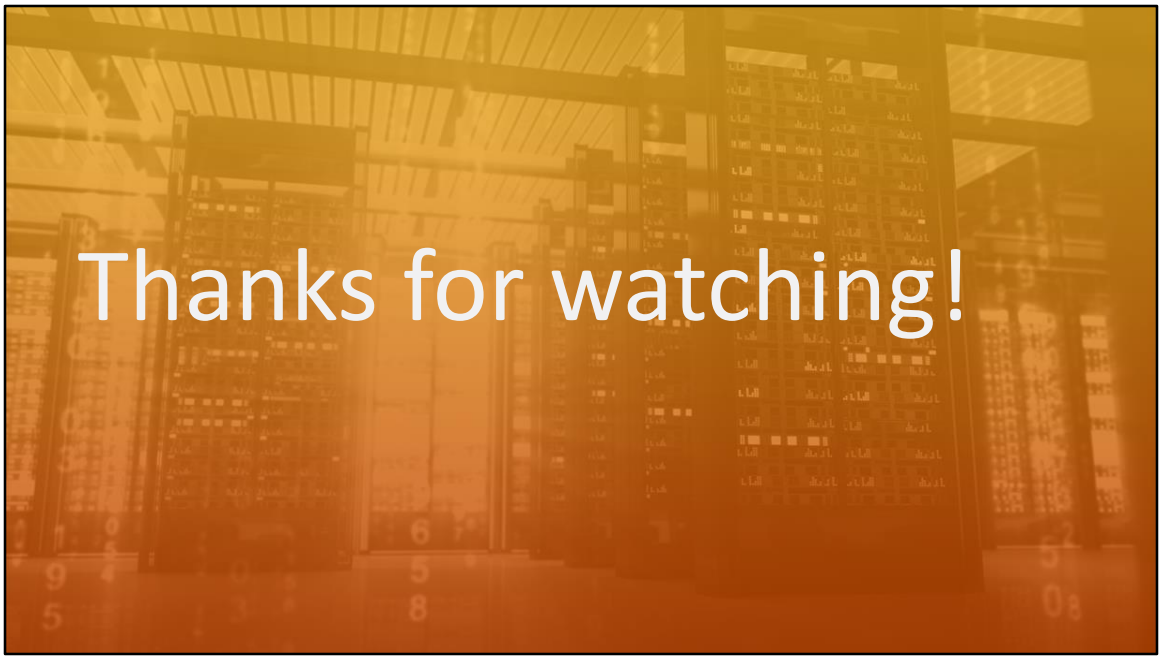
https://t.me/learningnets

Other Good Resources

- https://knowledge.digicert.com/solution/SO18140.html#AKI
- https://tools.ietf.org/html/rfc5280
- https://knowledge.digicert.com/solution/SO4583.html

Copyright © www.ine.com

https://t.me/learningnets



https://t.me/learningnets