7.5.8 Extended Validation Facts

This lesson covers the following topics:

- Extended validation
- Certificate formats
- Public key cryptography standards

Extended Validation (EV)

The most common use of certificates is for websites using Secure Socket Layer (SSL) or Transport Layer Security (TLS). These certificates prove to the user that the site is legitimate and trustworthy. When visiting a website that has been issued a certificate, the user sees a lock icon in the address bar. The user can click the lock to view the certificate information.

The highest level of these certificates is the Extended Validation certificate. The CA conducts a thorough and standardized identity verification process before issuing an Extended Validation certificate. This process includes the applicant proving:

- Exclusive rights to the domain.
- The organization's legal, physical, and operational existence.
- The organization's authorization for the issuance of the certificate.

Extended validation certificates can take up to 5 days to be issued.

Certificate Formats

The X.509 standard defines the format for SSL certificates. The following table shows the more common formats:

Certificate X.509 Format	Description
Distinguished Encoding Rules	Distinguished encoding rules (DER), is one of the older formats used. DER characteristics are: ▪ DER is a set of rules that defines how data must be encoded in a file. ▪ DER is defined by the ASN.1 standard. ▪ DER is a binary (non-text) encoding format. ▪ DER is mainly used in Windows systems. ▪ DER certificates usually have a .der or .cer file extension.
Privacy-Enhanced Email (PEM)	PEM certificates are the most common certificates in use. PEM was originally created to securely encode emails, but S/MIME and PGP quickly replaced it. The format PEM uses is perfect for encoding certificates. ▪ PEM certificates are base64 DER formatted. This means the binary information is encoded into ASCII text. ▪ The ASCII text is sandwiched between a header and footer that identify the data type. Common identifiers are:

	▪ CERTIFICATE ▪ CERTIFICATE REQUEST ▪ PRIVATE KEY ▪ X509 CRL ▪ A single PEM certificate can contain the intermediate certificate, root certificate, and private key. ▪ PEM certificates can have a .pem, .crt, .cer, or .key file extension.

Public Key Cryptography Standards PKCS)

PKCS is a group of standards published by RSA Security. These standards were published to promote the use of the cryptography techniques, such as the RSA algorithm, and several others.

Standard	Description
Public Key Cryptography Standards #7 (PKCS #7)	The PKCS #7 standard is used to format certificates and has the following characteristics: ▪ Is also known as the Cryptographic Message Syntax (CMS) standard. ▪ Is based on the PEM standard. ▪ Can contain only the intermediate certificate and root certificate, but not the private key. ▪ Is mainly used with digital signatures. ▪ Uses a file extension of .p7b or .p7c.
Public Key Cryptography Standards #12 (PKCS #12)	The PKCS #12 standard is also used to format certificates. It has the following characteristics: ▪ Is also known as the Personal Information Exchange Syntax Standard. ▪ Is based on the PEM standard. ▪ Holds certificate chains and the private key. ▪ Protects certificates and private keys with a password. ▪ Uses a file extension of .pfx or .p12.