

shell model: all certificates leading up to ^{and including} a trusted root must still be valid at the time of validation

hybrid model: certificate is valid if issuer was valid at time of issuance

chain model

extensions: may be critical or non-critical

if extension/attribute unknown: critical = invalid
non-critical = valid