Server-based Certificate Validation Protocol
Digital Certificate and PKI

- A public-key certificate is a digital certificate that binds a system entity's identity to a public key value, and possibly to additional data items.
  - "The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the CA which issued it" - RFC 2828

- A PKI is the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.
Certificate chain

Hierarchical PKI

Root CA

CA₁

CA₁₁

EE₁₁₁

CA₁₂

EE₁₂₁

CA₂

EE₂₁

CA₃

CA₃₁

EE₃₁

EE₃₁₁
Certificate validation

- A certification path is an ordered sequence of public-key certificates ending in a trust anchor.
- Certificate validation involves **discovering** and **validating** a certification path.
- It ensures that all certificates in that path are conformant to a certain set of rules (e.g., they have not expired or been revoked).
Certificate validation’s issues

- it is a complex process
- if cert handling is to be widely deployed in a variety of apps and environments
  - the amount of processing an application needs to perform before it can accept a certificate needs to be reduced
- apps need:
  - confirmation that the public key belongs to the identity named in the certificate
  - confirmation that the intended key can be used for the intended purpose
  - an efficient method of constructing a valid certification path
a simple certificate validation algorithm

START

Initialization

Process certificate

Last certificate in the path

yes

Wrap up for certificate validation

STOP

no

Prepare for next certificate
SCVP purposes

- It allows a client to delegate certification path construction and certification path validation to a server.
  - A common point of trust within the PKI.
- Certification path construction or validation is performed according to a validation policy, which contains one or more trust anchors (e.g., CA certs).
  - This enforces uniformly the rules and policies of a specific PKI (useful for centralized environments).
- It allows simplification of client implementations and use of a set of pre-defined validation policies.
Validation policy

- a set of rules and the adjacent parameters against which the validation of the certificate is performed by the server
  - SCVP path construction and validation are done in conformity with a validation policy
- SCVP clients can either reference parts of or full policies to be used for validation by the server
- the server will publish these policies to all potential clients, identifying these policies by means of OIDs (object identifiers)
Types of SCVP responders

- **untrusted**
  - can provide clients with certification paths and revocation information (e.g. CRL, OCSP responses) needed for the validation of the certification path

- **trusted**
  - can perform certification path construction and validation for the client
Trusted SCVP responders

- the client does not want to incur the overhead of including certification path validation software and running it for each certificate it receives (e.g. PDAs, smart-phones)
- the client is in an organization or community that wants to centralize management of validation policies
  - these policies might dictate that particular trust anchors are to be used and
  - the types of policy checking that are to be performed during certification path validation