

Extended Validation Models in PKI



Alternatives and Implications

Marc Branchaud

marcnarc@rsasecurity.com

John Linn

jlinn@rsasecurity.com



Overview

- Existing PKI practices
- Delegated path processing
- Cross-domain delegated validation
- Implications and future directions
- Conclusions

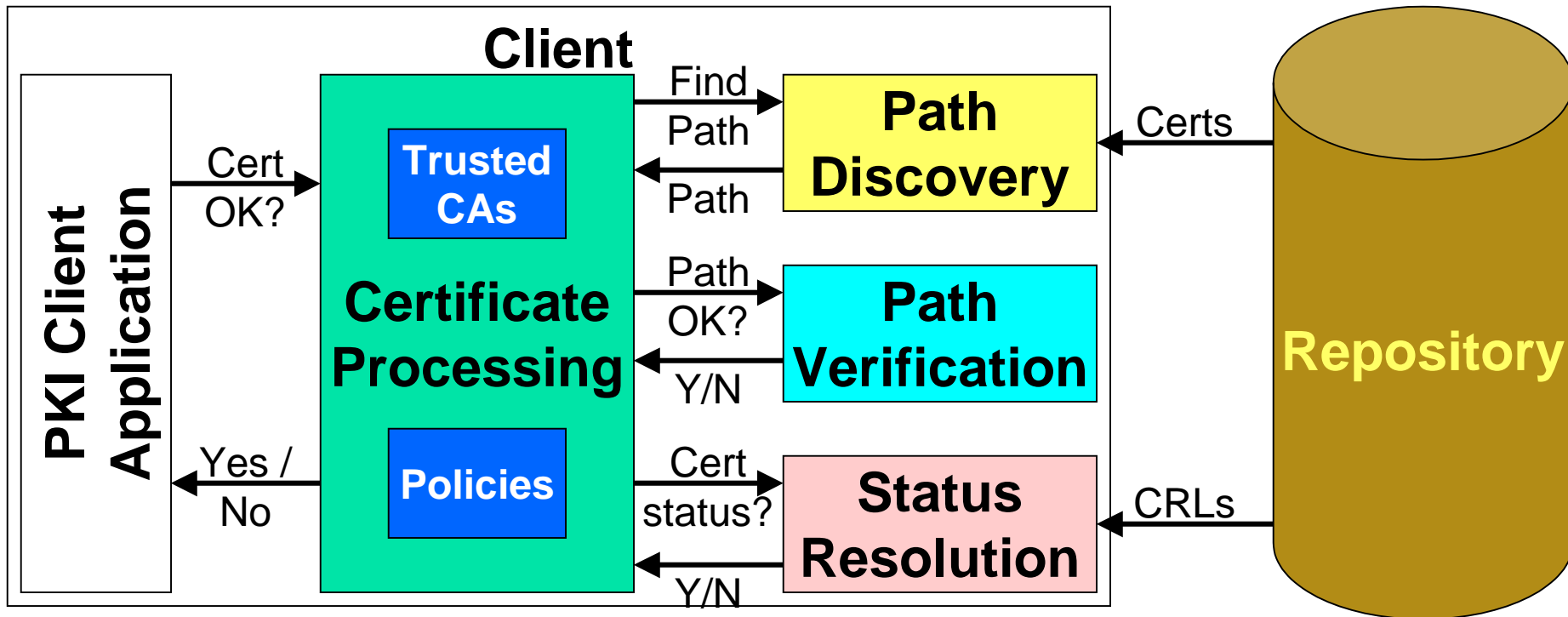


Existing PKI Practice: CRLs

- Original assumptions
 - Online, untrusted Directory as repository
 - Intermittent inter-site connectivity
 - Trusted authorities (CAs) kept off-line
- Path discovery & validation is client-based, using data from repository and messages
- Limitations include timeliness, large volumes of data to manage and transport

Traditional PKI

- Clients do all the work



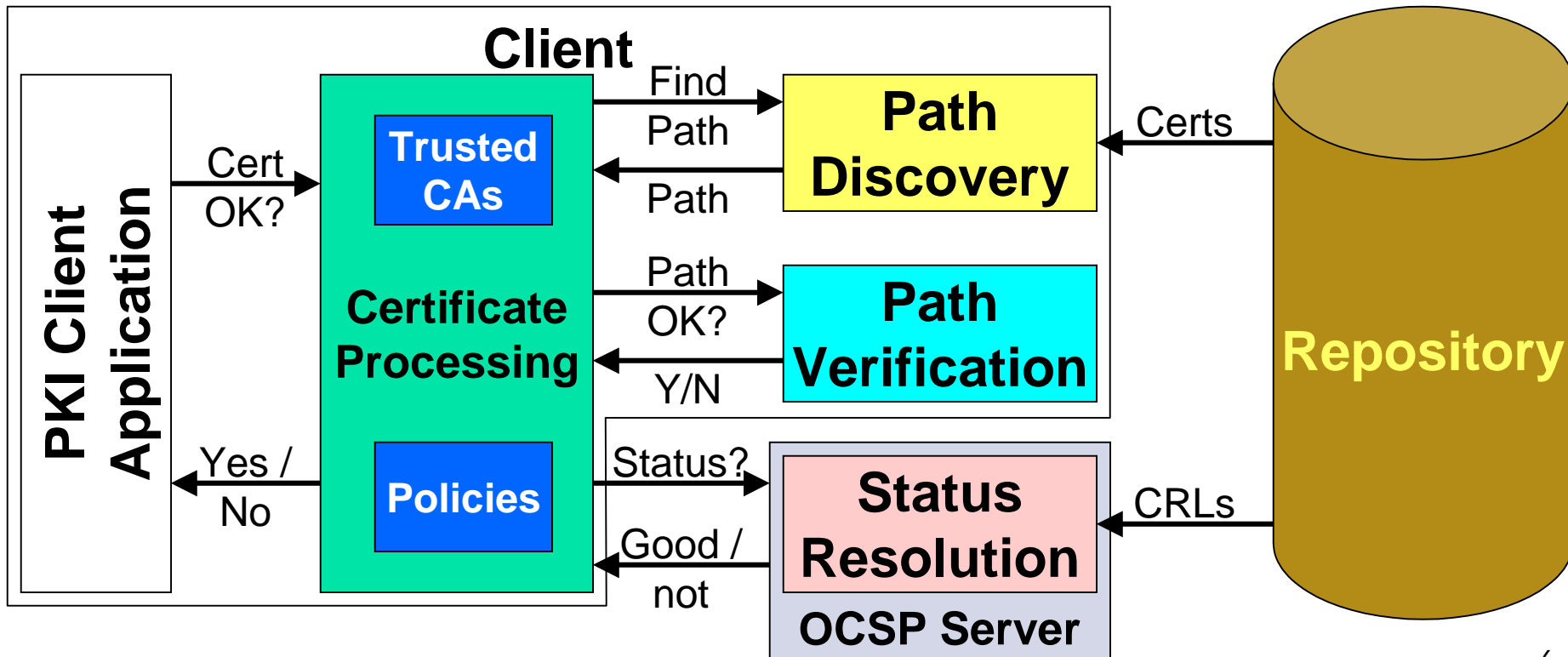


Existing PKI Practice: OCSP

- OCSP is seeing widespread adoption
- CAs delegate to OCSP responders that provide signed revocation information
 - Designed to enable migration from CRLs
 - Preserves client-based processing model, many semantics
 - Allows improved timeliness
 - Scope constrained to revocation status, not full validation of certificates or paths

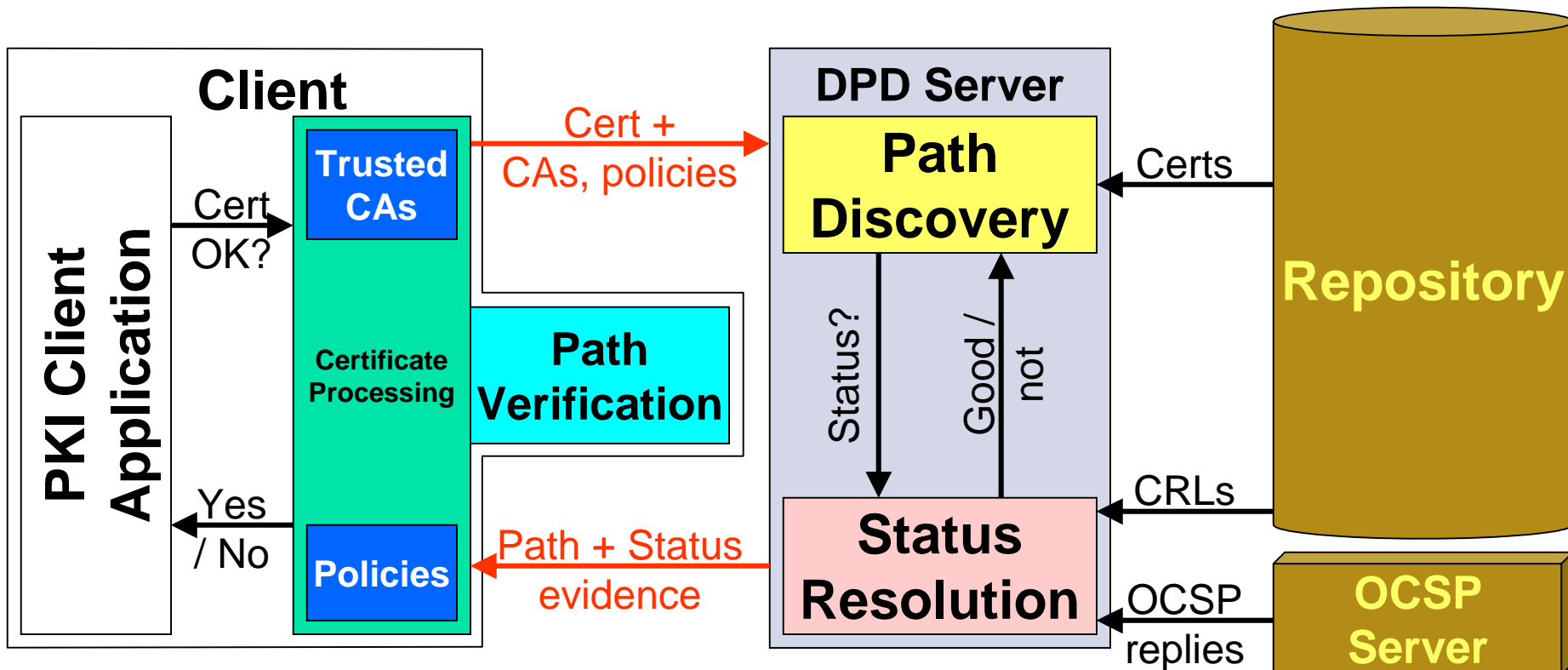
Online Certificate Status

- Clients no longer have to manage status



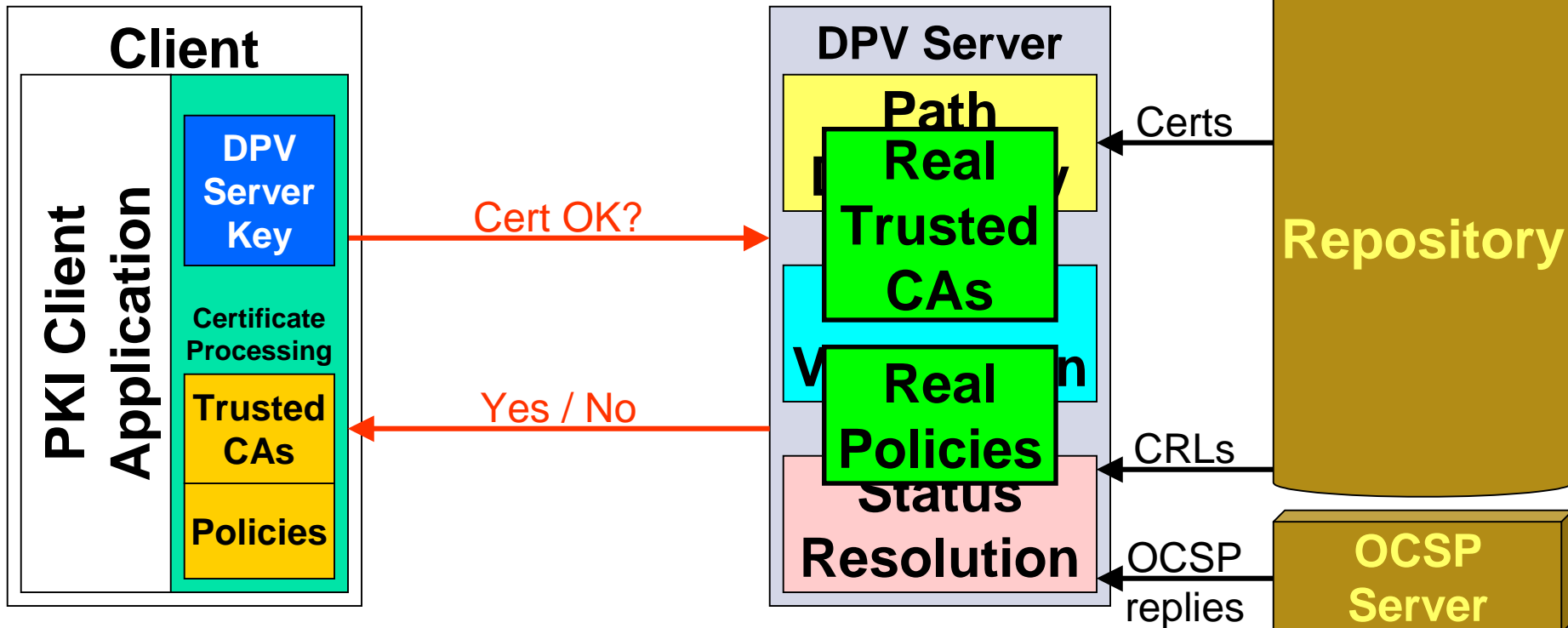
Delegated Path Discovery

- Clients no longer have to discover paths



Delegated Path Validation

- Current DPV proposals are to offload verification too





Delegated Path Validation

- Advantages of DPV model:
 - Vastly simpler client applications
 - Centralized domain administration
- Disadvantages of DPV model:
 - Online → availability & security issues
 - Convenient monitoring point (privacy)



Trust and DPV

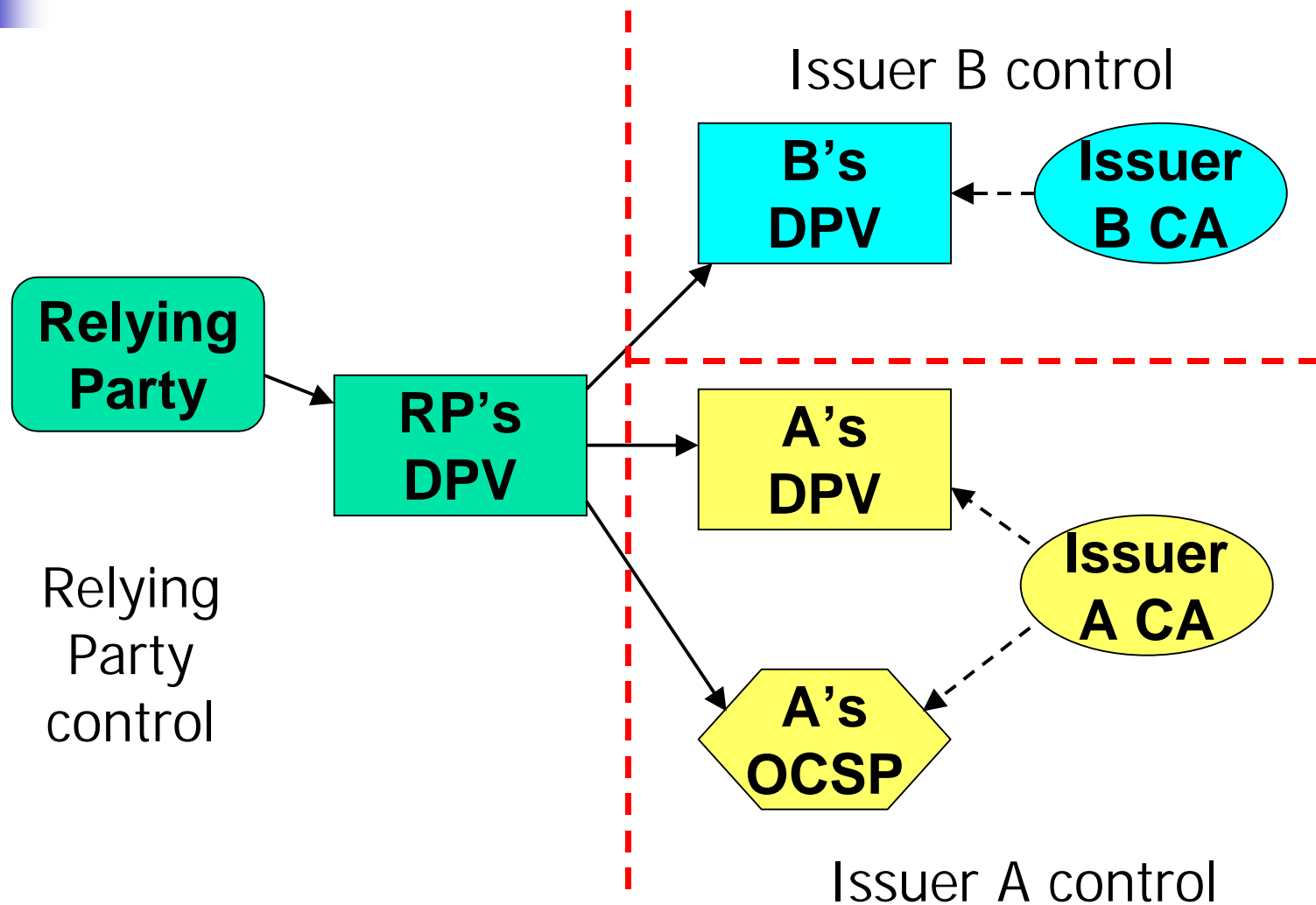
- The DPV server is the trust anchor
 - Easier to manage authority compromise
- The DPV server is the trust dictator
 - Clients do not validate the server's "correctness"
 - Client inputs are merely hints
 - Still useful for client to identify context



Delegating Trust Across Domain Boundaries

- DPV servers consult other domains' services to build responses to queries
 - Clients rely on their DPV server to select the right sources to validate arbitrary certificates
 - Different DPV servers' views may differ
- Validation combines issuer domain information (certificates and status) with RP domain policies

Delegated Validation Across "Trust Fronts"





Forms of Delegated Validation

- **Chained:**

- Client gets authoritative reply via intermediary
- Intermediaries on path may be included

- **Referred:**

- Clients redirected to authoritative server
- Responses may be traceable to it

- **Recursive:**

- Each server aggregates data and generates its own responses
- Limited traceability



DPV Implications for Cross-Certificates

- Domains can consider inter-domain trust relationships in formulating their DPV responses
- Fine-grain activation of trust relationships
 - Available only for some clients
 - Available only in some circumstances
 - Like having multiple cross-certificates between domains



DPV Implications for Revocation

- Path construction actively involves intermediate domains
- Domains can consider status in formulating their responses
- No need to explicitly query for status
 - Status is simply another factor in the availability of certain paths
 - There is no path to a revoked certificate



DPV Implications for Certificates

- Queries eventually reach the issuer
 - Necessary to obtain certificate status
- Issuer can assert more than just status
 - Could respond with individual certificate elements, e.g.:
 - Subject's DN changes after cert is issued
 - Can return new DN in DPV response
- Could even return subject's public key
 - No revocation publishing at all



DPV Implications for Certificates

- In the limit, certificates become obsolete
- Certificate-free PKI:
 - Authorities assign identifiers to entities' public keys
 - Entities present identifiers instead of certs
 - RPs resolve identifiers to public keys via fully-delegated DPV
 - XKMS already supports URLs for keys
- Active assertions are a new paradigm for PKI – X.509 didn't consider them



Conclusions

- Current trend towards simplifying PKI clients challenges basic assumptions
- Delegating trust & distributing validation creates active authorities and intermediaries
 - Introduces new issues: availability, latencies
 - Facilities to constrain trust gain prominence
- Implications for revocation, certification
- Caveat adopter!