Distributed Path Validation

Massive Scalability for Federated PKIs
Road Map

• Path Validation
• Path Discovery
• Revocation Checking
• Delegated Path Validation (DPV)
• Delegated Path Discovery (DPD)
• CoreStreet’s Distributed DPD
What is Path Validation?

**Does a path exist?**
1. From something I trust
2. To the subscriber’s certificate
3. With no revoked certificates
4. That satisfies all policies/constraints

To: Colin
Signed: Donald
What is Path Discovery?

Find a chain of certificates from something I trust explicitly:

to a subscriber’s certificate:

To: Richard

Signed: Donald

CN = Donald Rumsfeld
Easy: Simple Hierarchy

DoD Class 3 Root

Issuer: DoD Class 3 Root
Subject: DoD Email CA-3

DoD Email CA-3

Issuer: DoD Email CA-3
Subject: Donald Rumsfeld

Donald Rumsfeld

To: Richard

Signed: Donald

© Copyright 2004 CoreStreet, Ltd.
Hard: Cross-Certs and Bridges

To: Colin
Signed: Donald

© Copyright 2004 CoreStreet, Ltd.
Hard: Cross-Certs and Bridges

DoD Class 3 Root

Issuer: FBCA
Subject: DoD Root

Federal Bridge CA

Issuer: State Dept. Root
Subject: FBCA

State Dept. Root

Issuer: DoD Root
Subject: DoD Email CA-3

DoD Email CA-3

Issuer: DoD Email CA-3
Subject: Donald Rumsfeld

Donald Rumsfeld

Relying party does not know about common root …

To: Colin
Signed: Donald
What is Revocation Checking?

Has a certificate been revoked by its issuer?

To: Richard

Signed: Donald
CRLs: Poor scalability

19 DoD CRLs (35MB) x 4 million clients = 120 Terabytes per day from directory service
CRLs: Poor performance

Need CRLs for all accepted certificates:
Federation explodes performance problem
OCSP: Certificate Validation Protocol

Responder

"Is this cert revoked?"

Issuer: DoD Email CA-3
Subject: Donald Rumsfeld

"No, it is not revoked."

Cert #1234: Good

To: Richard
Signed: Donald

© Copyright 2004 CoreStreet, Ltd.
OCSP: Market Acceptance

Native OCSP:
- Microsoft Windows (Longhorn)
- Identrus
- Netscape / Mozilla Communicator
- Sun ONE Identity Server
- RIM Blackberry PDA
- Compaq iPAQ
- Netegrity SiteMinder
- Oblix Netpoint
- Silanis Approvelt
- Arcot Adobe Acrobat signing
- Elock Assured Office
- IBM DSMS
- Ascertina PDF Signer
- Conclusive TrustLogic
- Lexign ProSigner
- Gemplus eSigner
- CMG WAP Gateway
- Cisco Local Director, VPN
- Netscreen VPN
- Cyberguard VPN
- VeriSign

OCSP libraries/plug-ins:
- CoreStreet
- Alacris
- ValiCert
- Ascertina
- AssuredBytes
- Kyberpass
- SyTrust
- RSA Keon and BSAFE
- Authentica

Plug-ins support:
- Microsoft Outlook
- MS Outlook Express
- MS Internet Explorer
- MS IIS
- Apache web server
- Netscape/AOL/Sun servers
- Microsoft VPN
- MS Office XP
- Eudora (via Authentica)
- Peoplesoft (via Authentica)
- SAP (via Authentica)
- Lotus Notes (via Authentica)
First-generation OCSP

Certificate Authority

CRLs

OCSP Responder

OCSP Requests

Clients

requires trust
(physical and data security)

© Copyright 2004 CoreStreet, Ltd.
Distributed OCSP

- Certificate Authority
- RTC Authority
- Pre-signed OCSP Responses
- Responders
- OCSP Response

**Principle:**
Separate security functions from distribution.

- Requires trust
  (physical and data security)
Distributed OCSP: Security

“Off-line” signing key prevents compromise

No keys in online servers; responders cannot "lie"
Distributed OCSP: Performance

1000+ requests/sec each:
- No RSA at runtime
- Simple table look-ups
- 10-100 ms per request
Distributed OCSP: Cost

Server: $3k
Management: $3-5k / year

~ $100k less per responder than First-generation OCSP
Distributed OCSP, Managed

RTC Authority

Pre-signed OCSP Responses

Responders

OCSP Response

requires trust
(physical and data security)
Distributed OCSP, Enterprise

RTC Authority

Responder Appliance 1400

© Copyright 2004 CoreStreet, Ltd.
Server-Assisted Path Validation?

Two approaches:
1. Delegated Path Validation (DPV)
2. Delegated Path Discovery (DPD)
Option 1: DPV

Vaulted server with private keys

CA certificates, CRLs, OCSP

“Can I trust this cert: if I trust this root?”

“Yes, you can.”

State Dept. Root

© Copyright 2004 CoreStreet, Ltd.
Local DPV Servers?

- High cost per server
- IT management burden
- Security risk
- Configuration management
Central DPV servers?

- **Huge** impact if compromised
- Performance (latency, …)
- $100,000+ per server/year
Path Validation Option 2: DPD

“Can I trust this cert: if I trust this root?”

State Dept. Root

Lightweight server, no keys

CA certificates and OCSP responses

Issuer: State Dept. Root
Subject: FBCA

FBCA: Good

Issuer: FBCA
Subject: DoD Root

DoD Root: Good

Issuer: DoD Root
Subject: DoD CA-7

DoD CA-7: Good

Issuer: D. Rumsfeld

D. Rumsfeld: Good
Distributed DPD

CAs → RTC Authority

Optimal cert paths, pregenerated OCSP responses

Responders

Standard OCSP & Certs

Clients

= requires trust (physical and data security)
D-DPD: Managed, Hybrid Options

RTC Authority

Responder Appliance 1400

© Copyright 2004 CoreStreet, Ltd.
DPD Server Demonstration

Cambridge, MA

RTC Authority

RTC Responder

Clients
Distributed DPD Advantages

- No online server key risk
- Massive scalability
- Low cost per server
- Managed service option
- Minimal IT impact
- Open standards
Contact Us

- To arrange for a demonstration or technical briefing, please contact either:
  - Fred Levy, flevy@corestreet.com, 301-528-0025
  - Randy Bowman, rbowman@corestreet.com, 301-254-3858