CoreStreet
REAL TIME CREDENTIALS

Distributed Path Validation

Massive Scalability for Federated PKIs

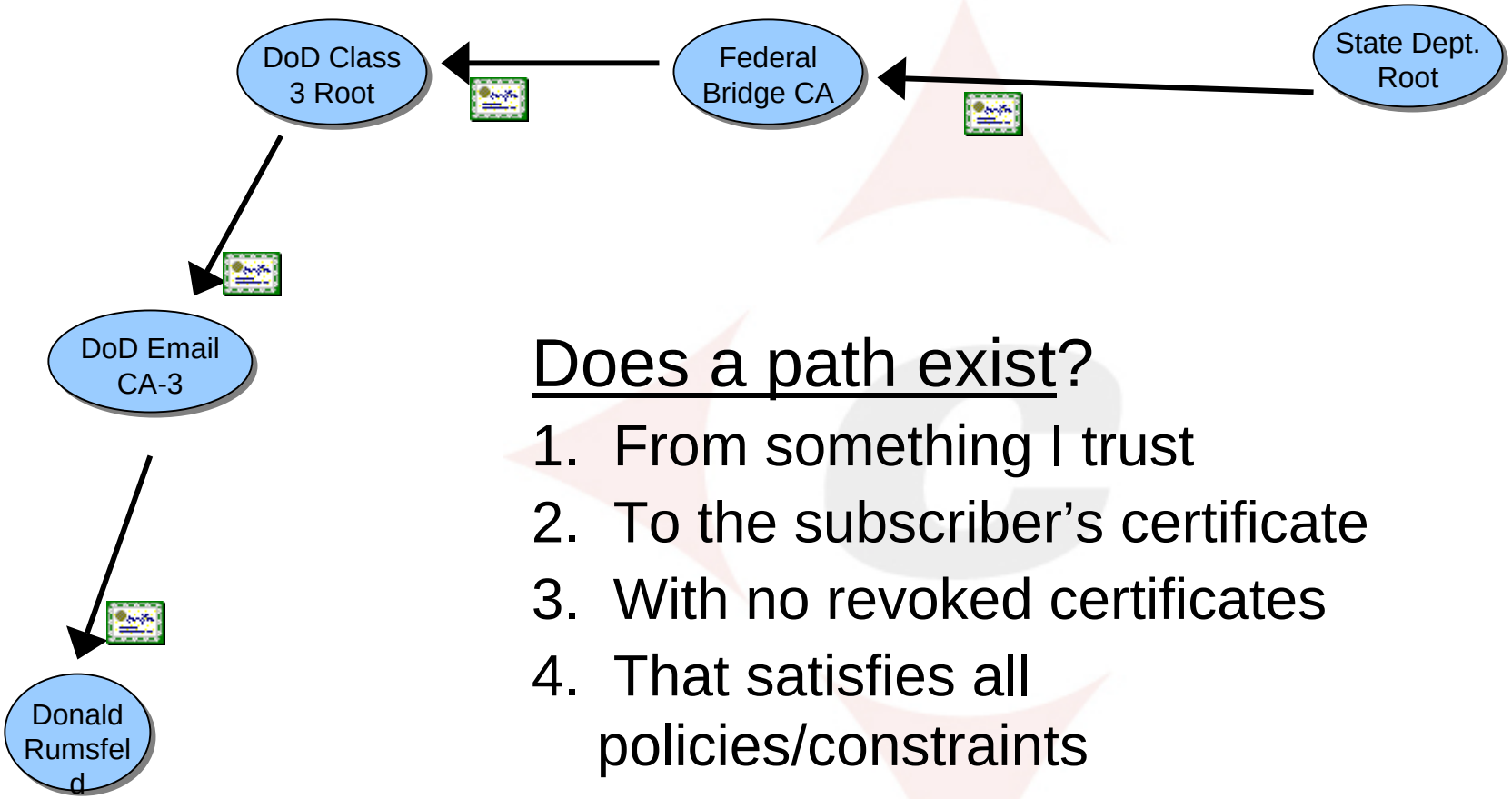
CoreStreet
REAL TIME CREDENTIALS

Road Map

- **Path Validation**
- **Path Discovery**
- **Revocation Checking**

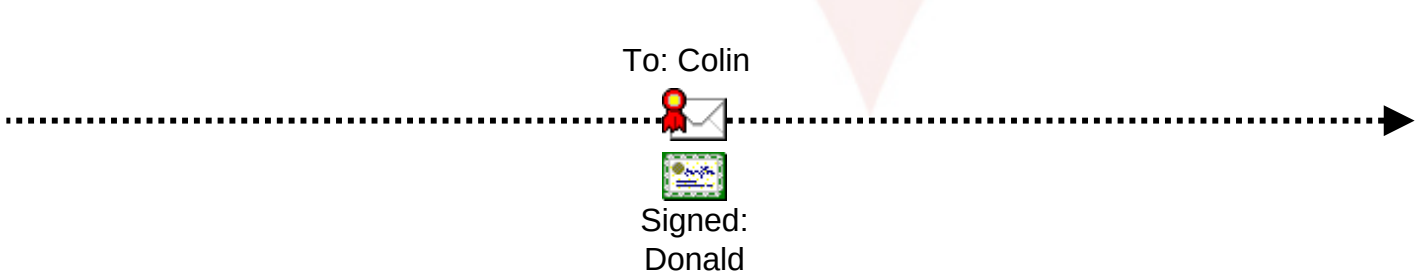
- **Delegated Path Validation (DPV)**
- **Delegated Path Discovery (DPD)**
- **CoreStreet's Distributed DPD**

What is Path Validation?

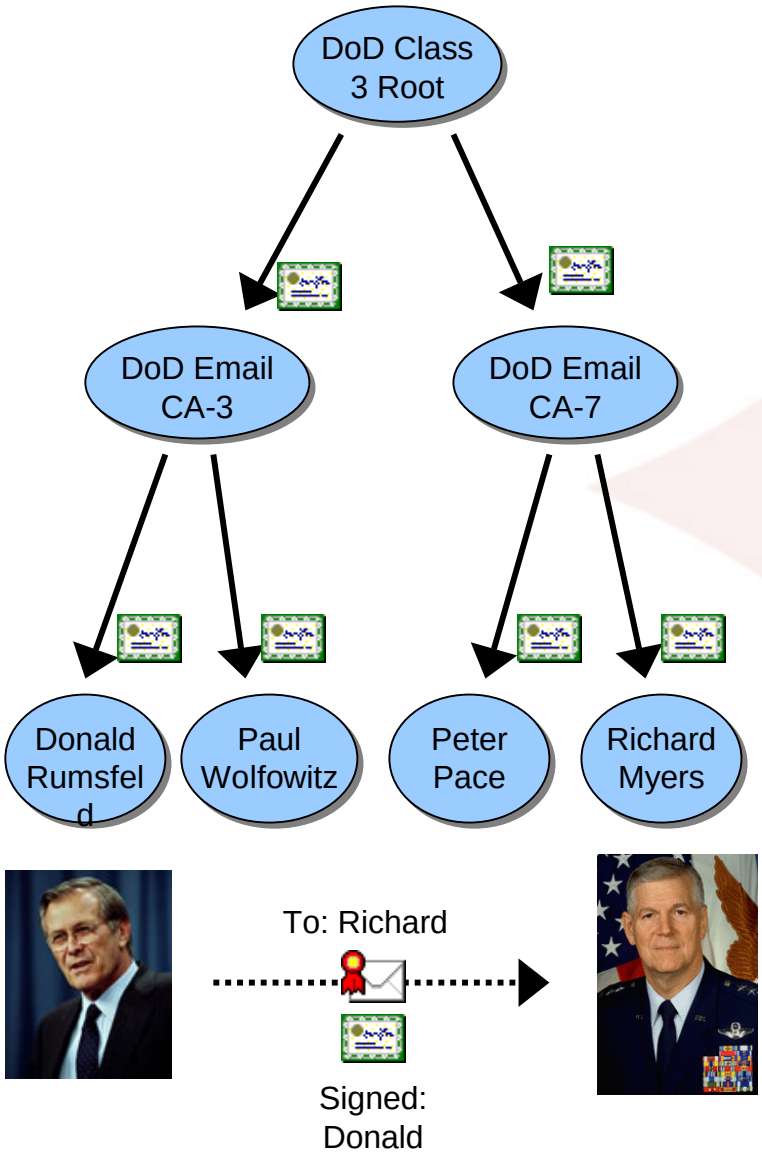


Does a path exist?

1. From something I trust
2. To the subscriber's certificate
3. With no revoked certificates
4. That satisfies all policies/constraints



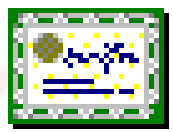
What is Path Discovery?



Find a chain of certificates from something I trust explicitly:

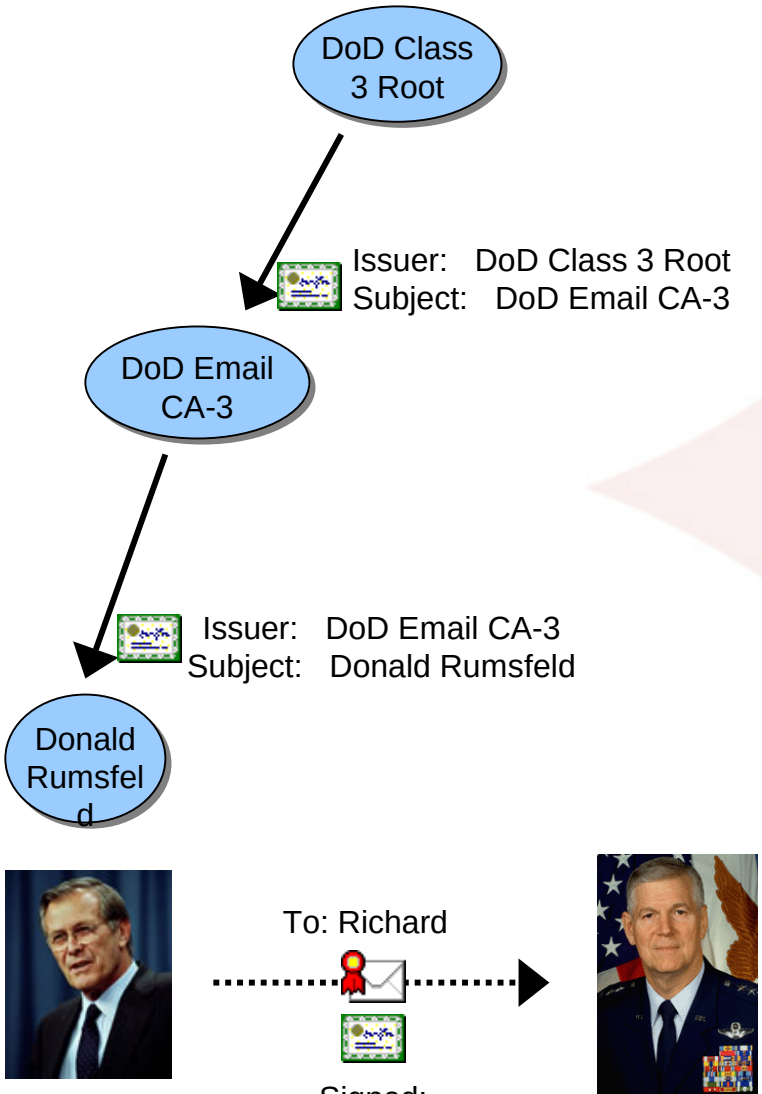
DoD Class 3 Root

to a subscriber's certificate:

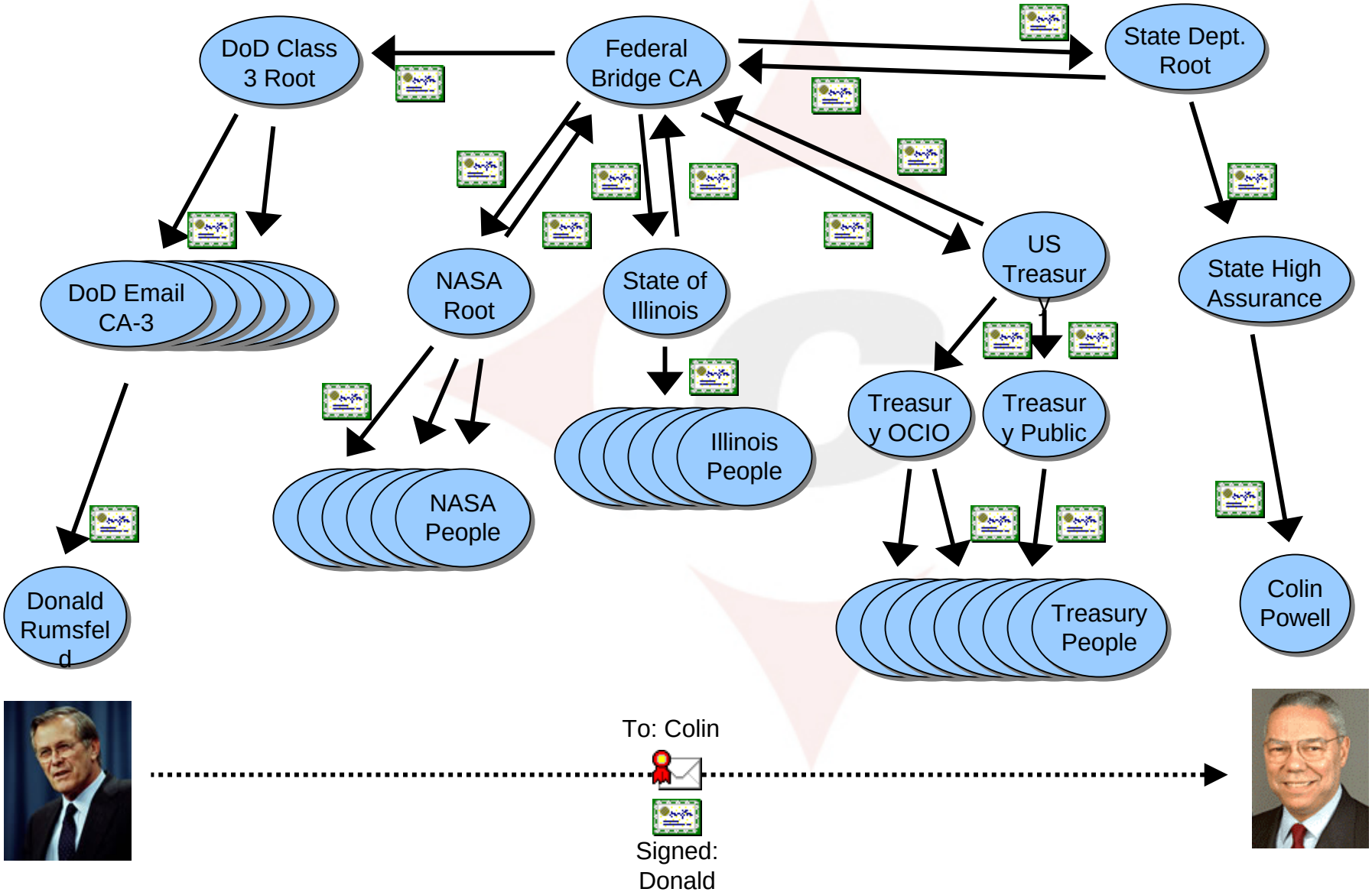


CN = Donald Rumsfeld

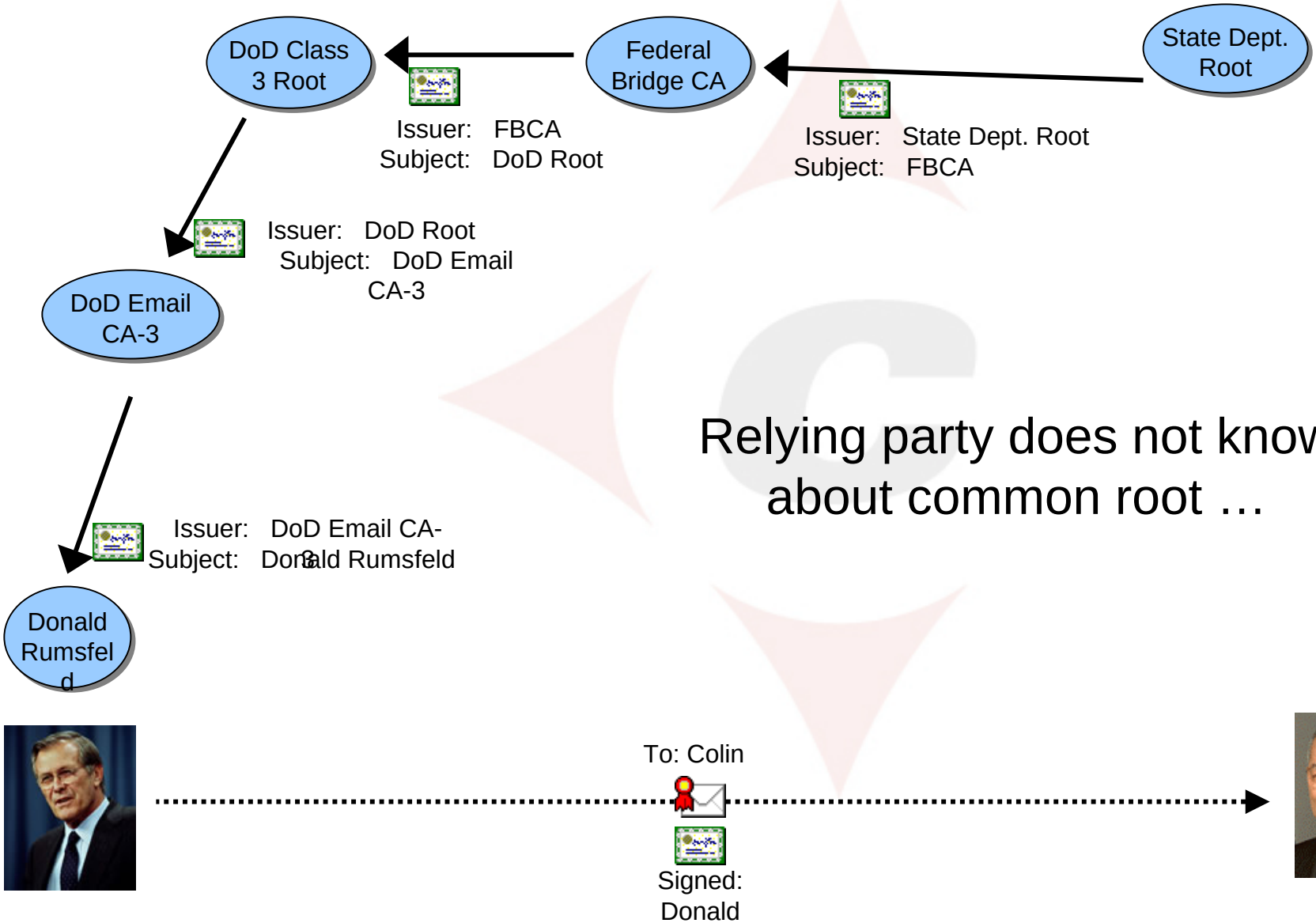
Easy: Simple Hierarchy



Hard: Cross-Certs and Bridges

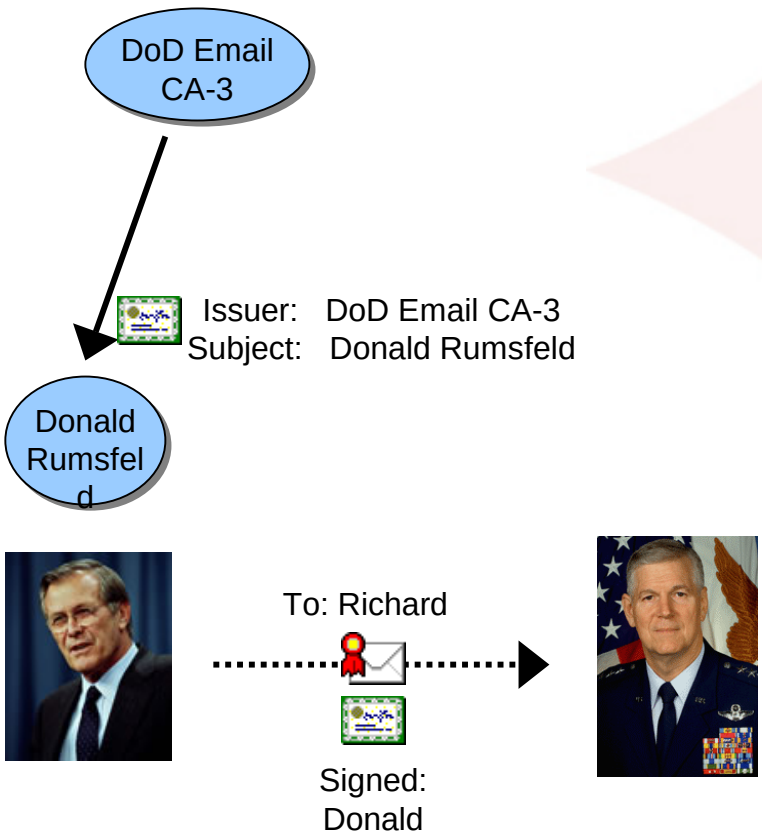


Hard: Cross-Certs and Bridges



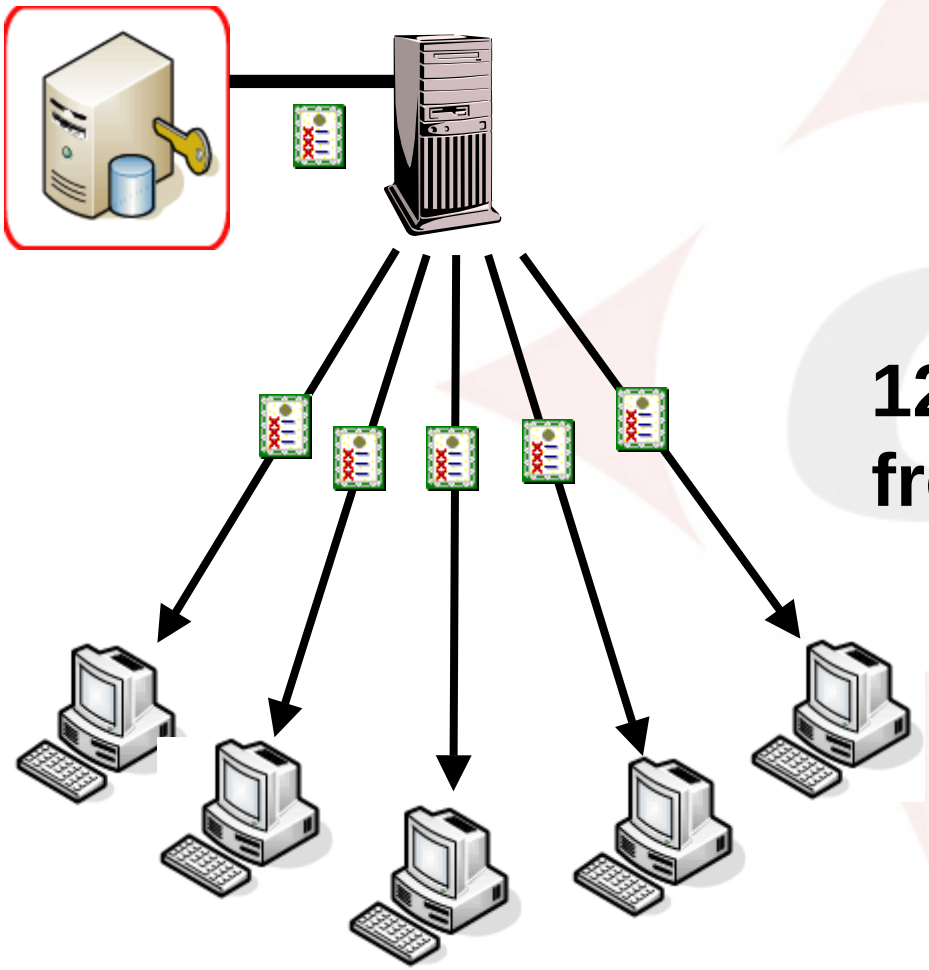
Relying party does not know about common root …

What is Revocation Checking?



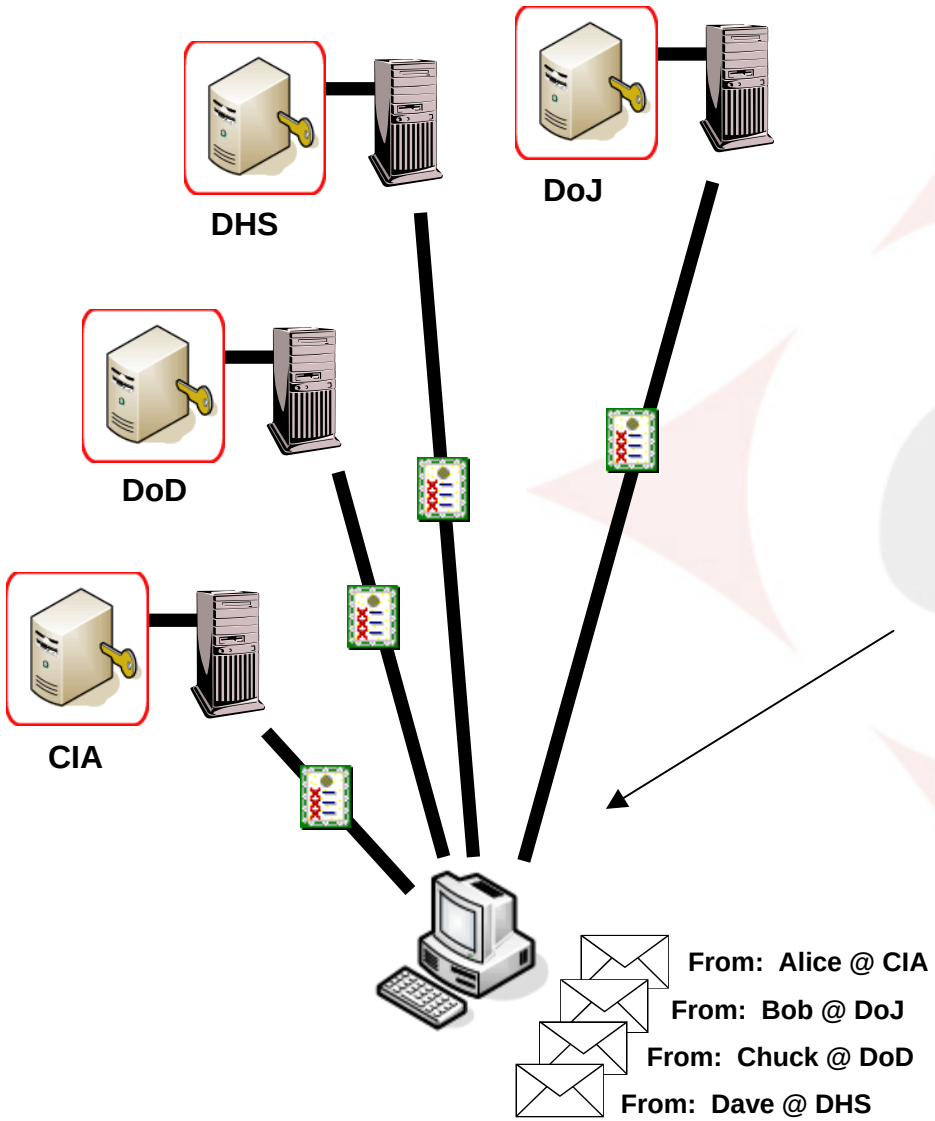
"Has a certificate been revoked by its issuer?"

CRLs: Poor scalability



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

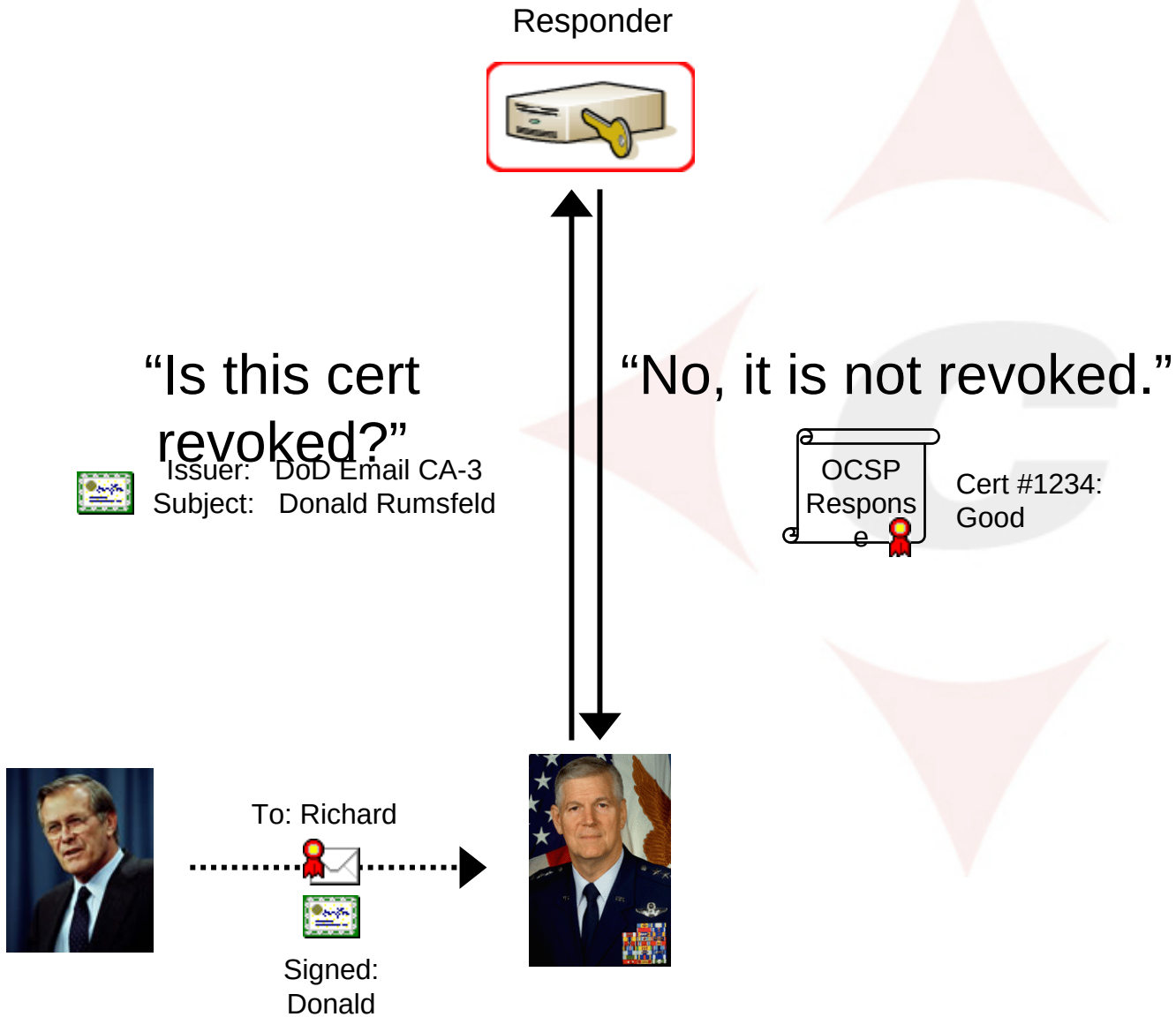
CRLs: Poor performance



Need CRLs for all accepted certificates:

Federation explodes performance problem

OCSP: Certificate Validation Protocol



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 ApproveIt
- 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

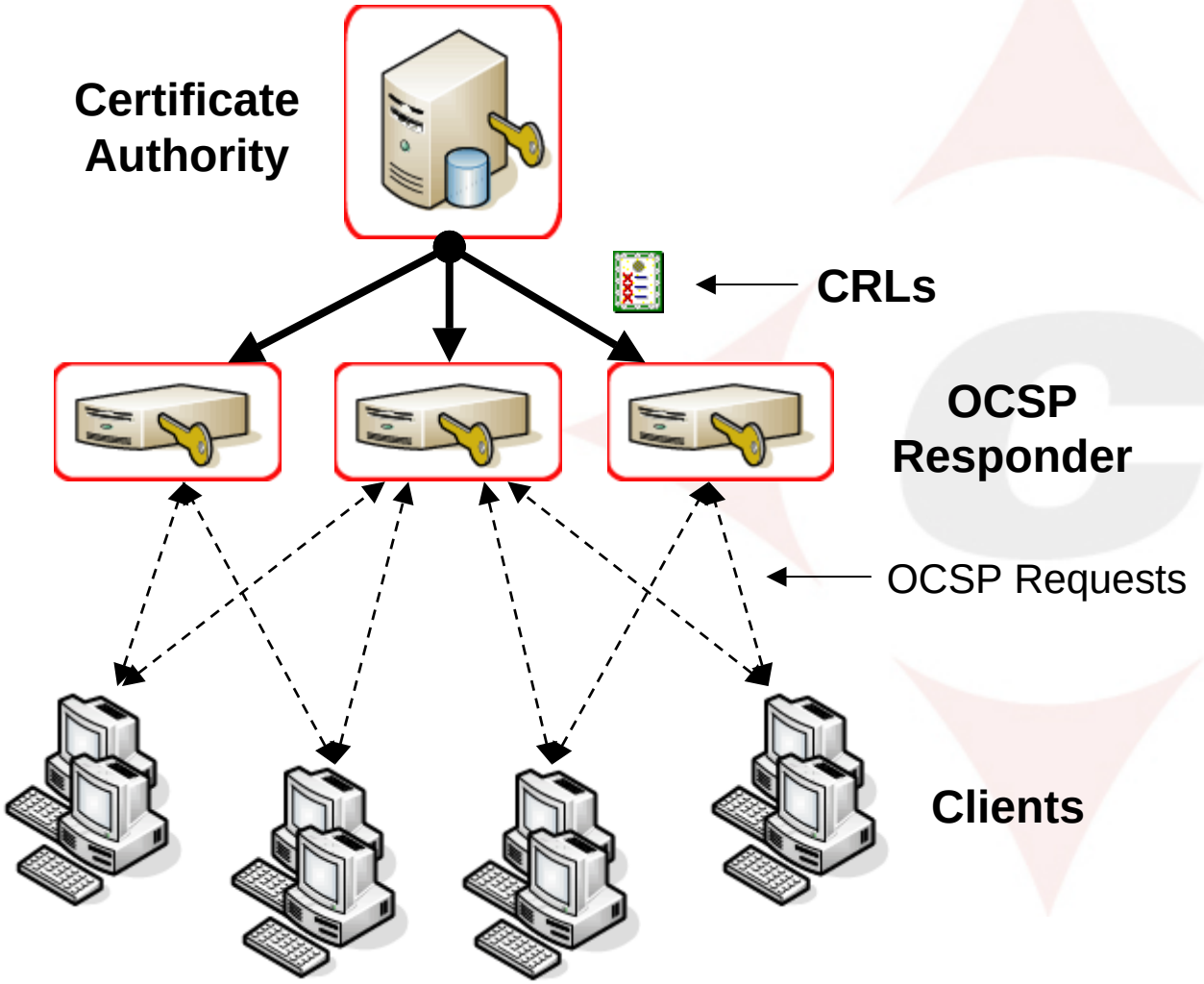
OCSP libraries/plug-ins:

- CoreStreet
- Alacris
- ValiCert
- Ascertina
- AssuredBytes
- Kyberpass
- SyTrust
- RSA Keon and BSAFE
- Authentica

Plug-ins support:

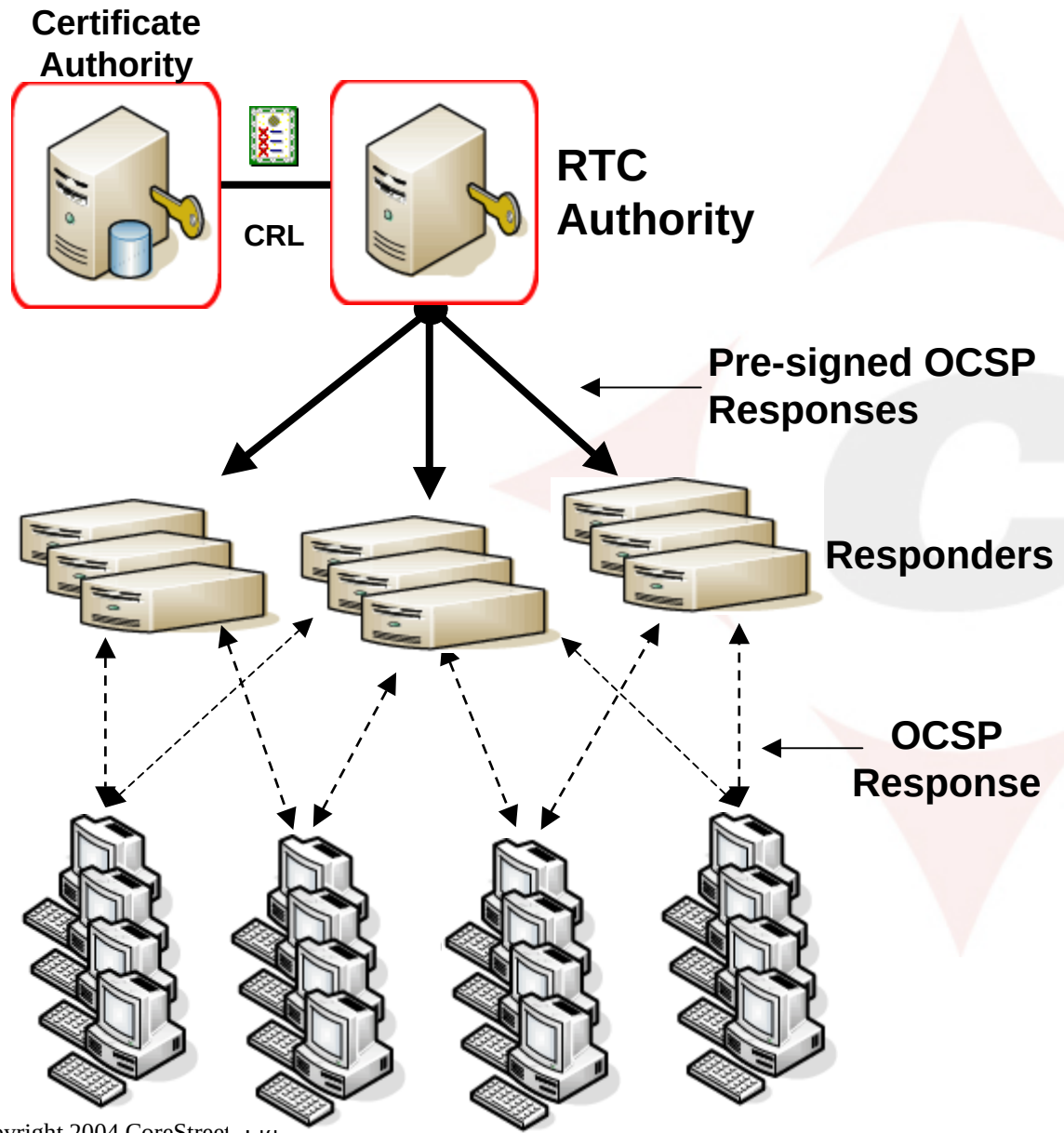
- Microsoft Outlook
- MS Outlook Express
- MS Internet Explorer
- MS IIS
- Apache web server
- Netscape/AOL/Sun servers
- Microsoft VPN
- MS Office XP
- Eudora (via Authentica)
- Peoplesoft (via Authentica)
- SAP (via Authentica)
- Lotus Notes (via Authentica)

First-generation OCSP



= requires trust
(physical and data security)

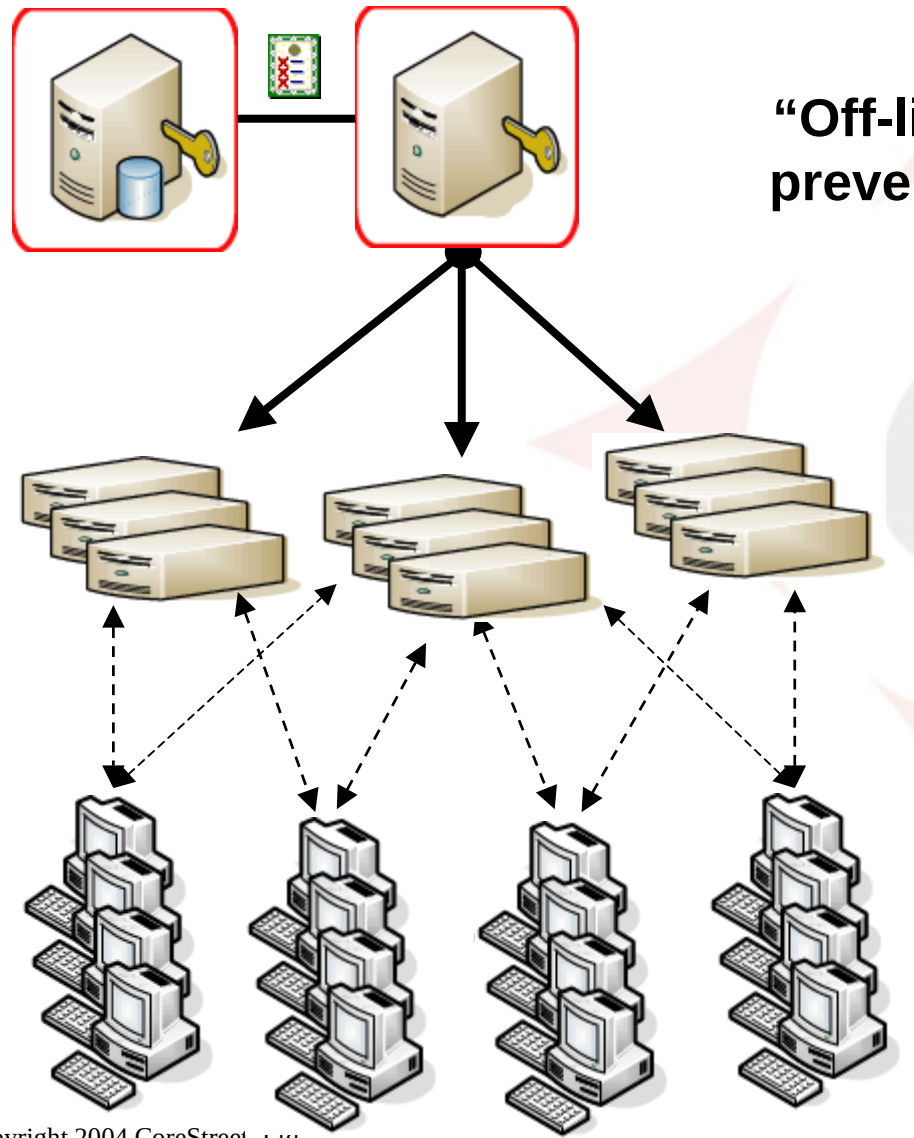
Distributed OCSP



Principle:
Separate security functions from distribution.

= requires trust
(physical and data security)

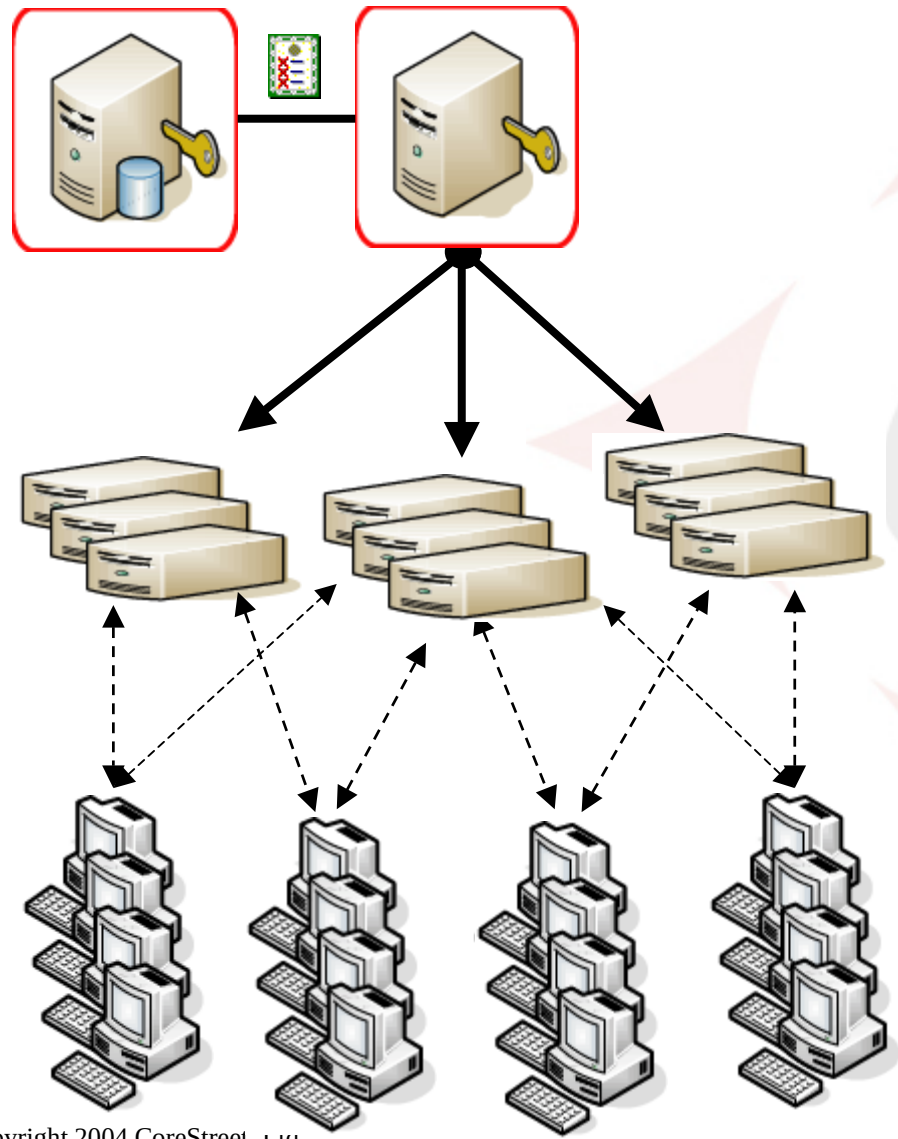
Distributed OCSP: Security



“Off-line” signing key prevents compromise

No keys in online servers; responders cannot “lie”

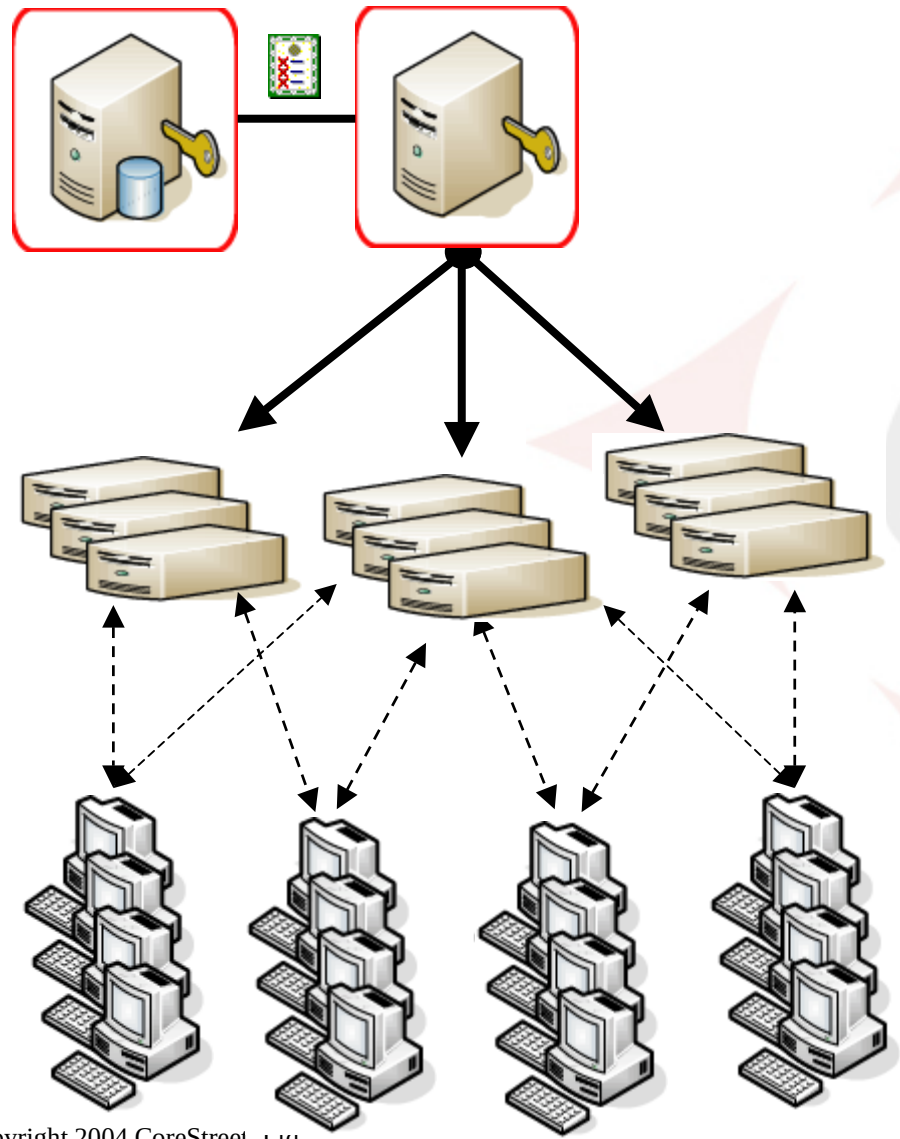
Distributed OCSP: Performance



1000+ requests/sec each:

- No RSA at runtime
- Simple table look-ups
- 10-100 ms per request

Distributed OCSP: Cost

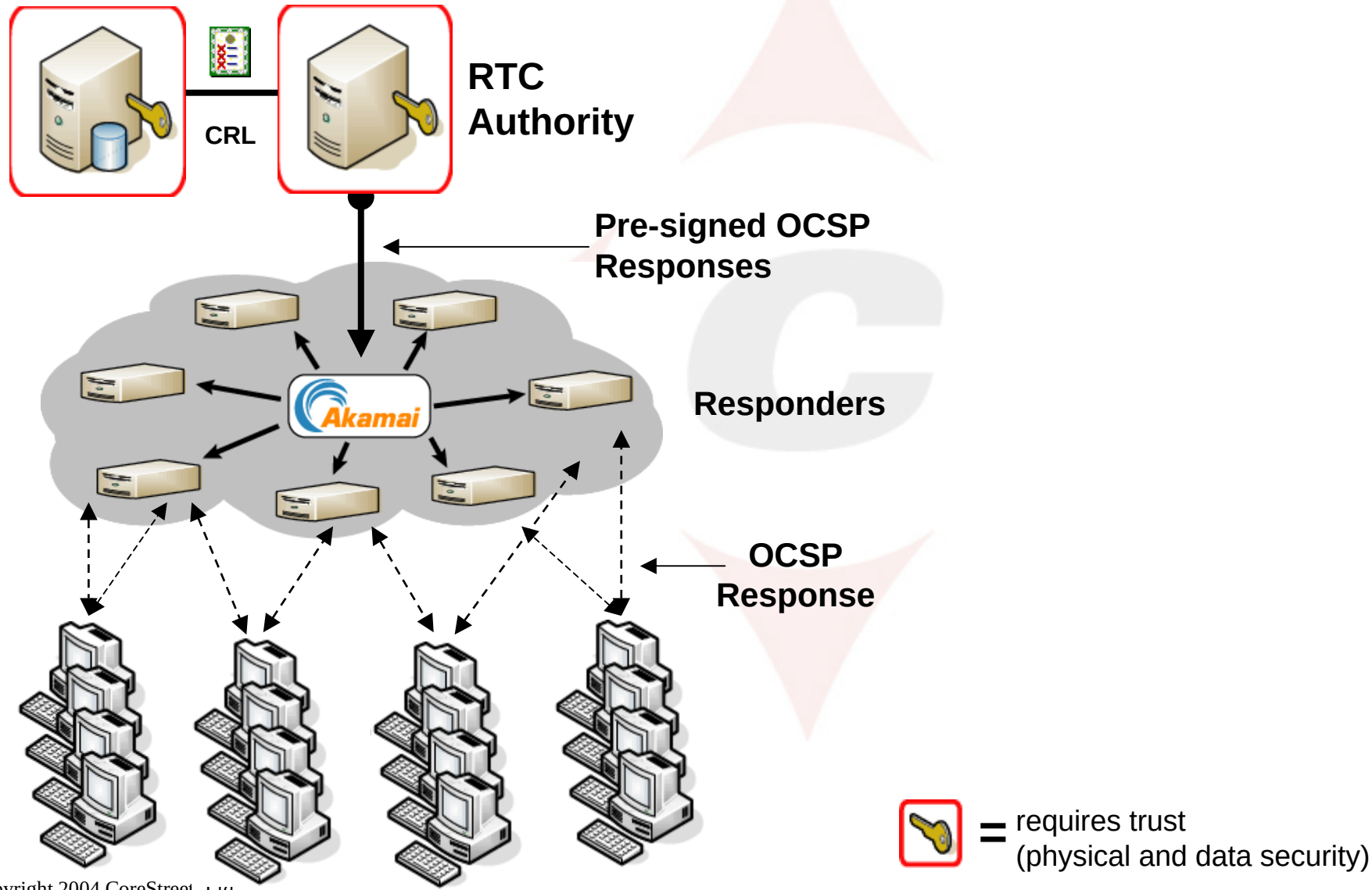


Server: $3k

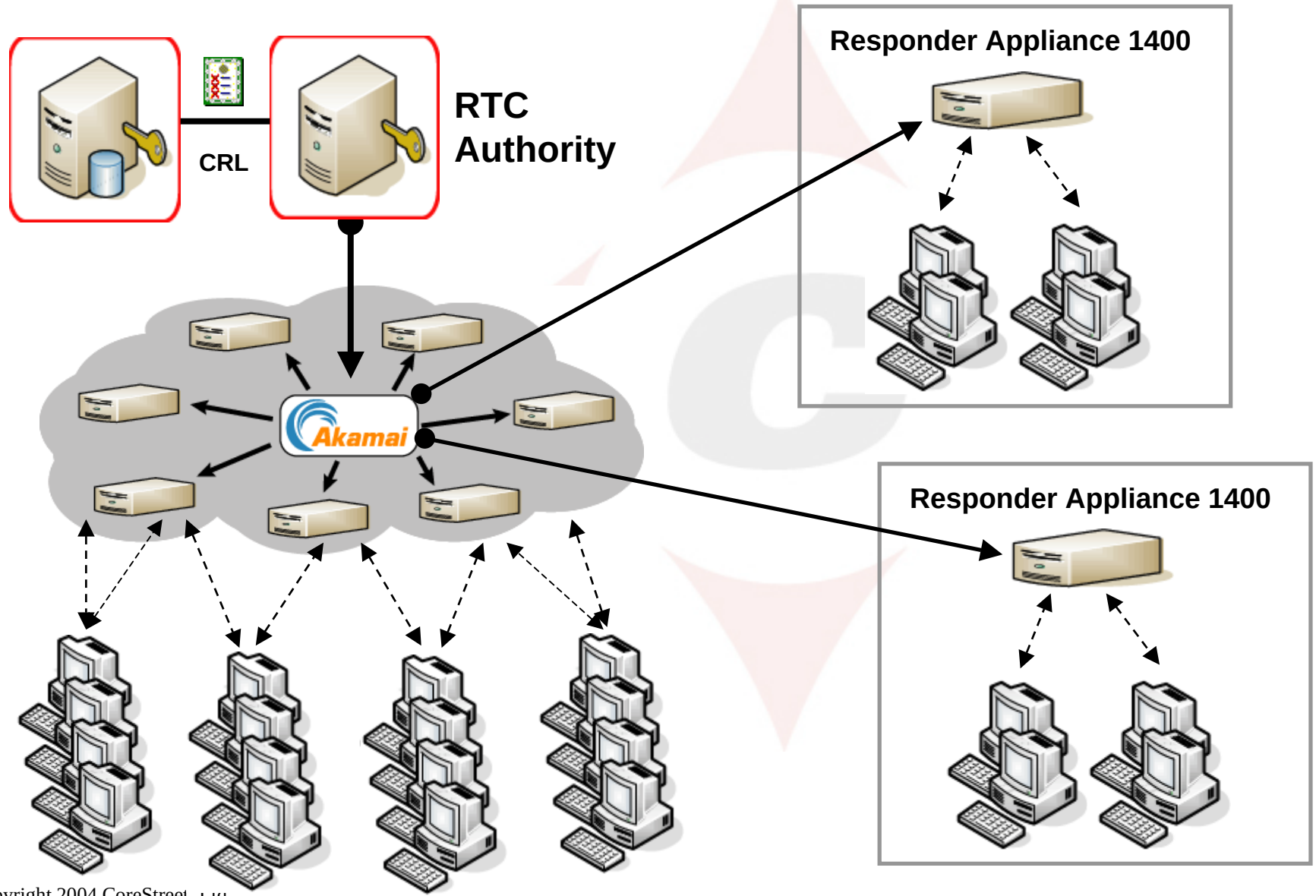
Management: $3-5k / year

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

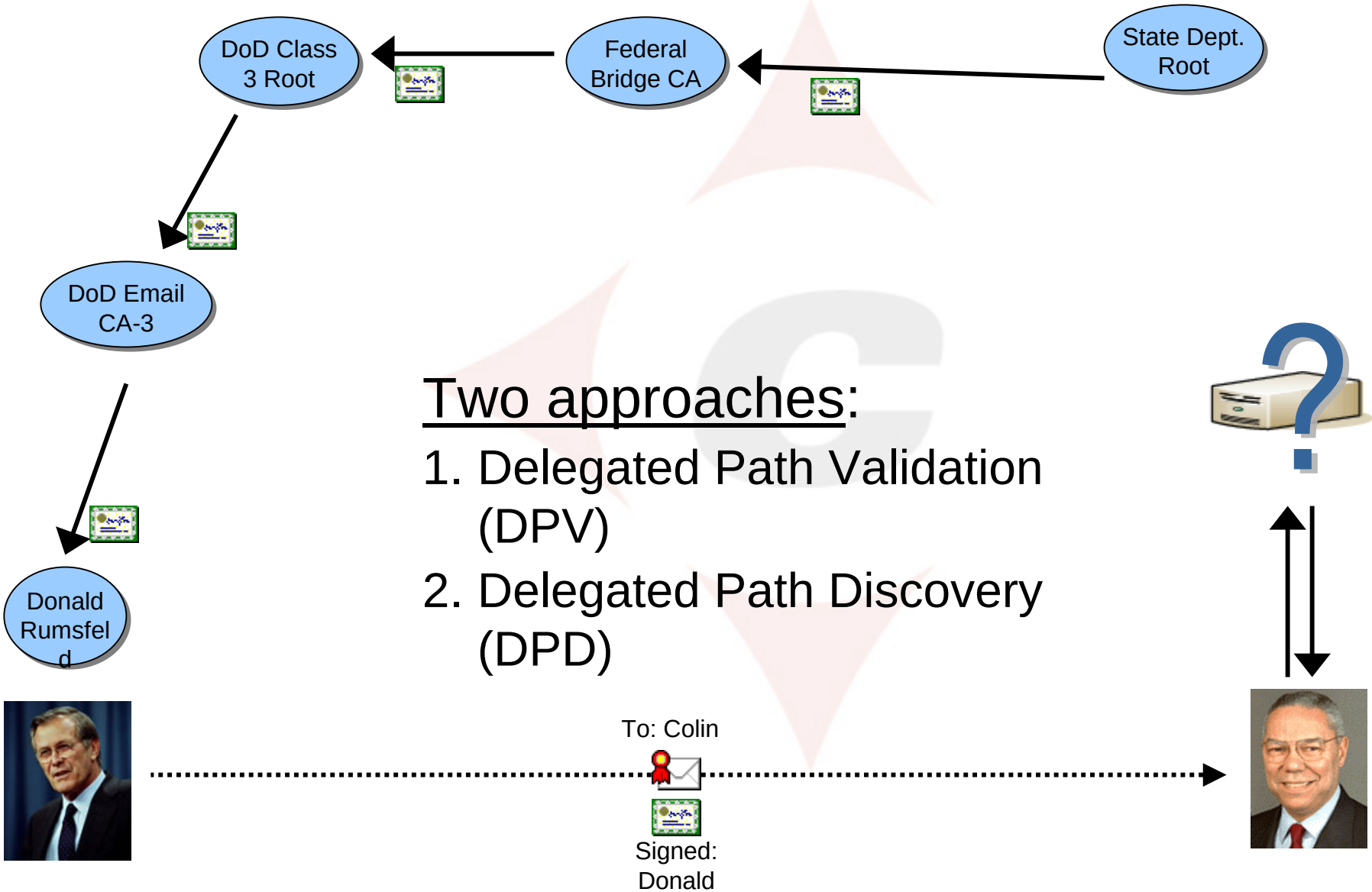
Distributed OCSP, Managed



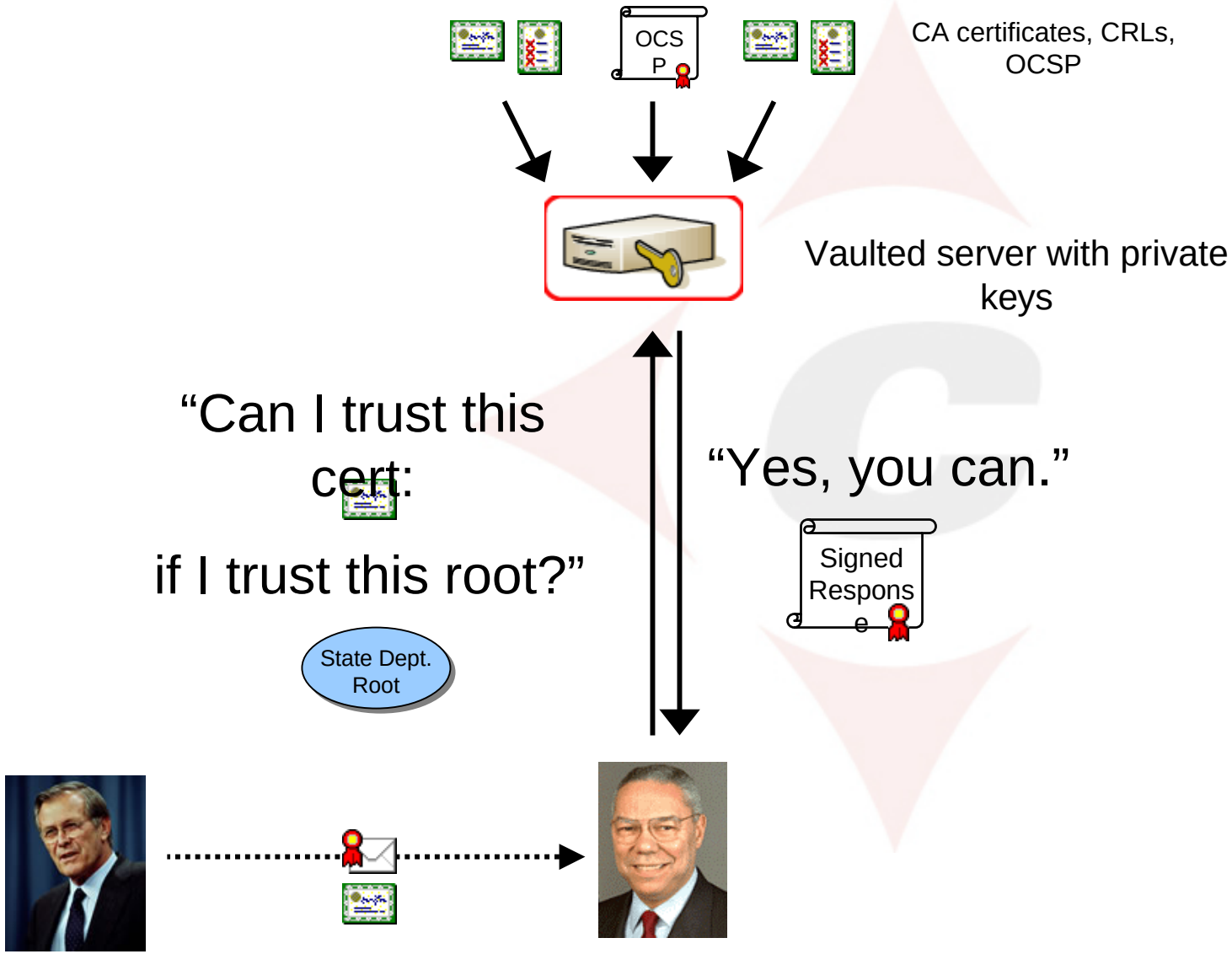
Distributed OCSP, Enterprise



Server-Assisted Path Validation?

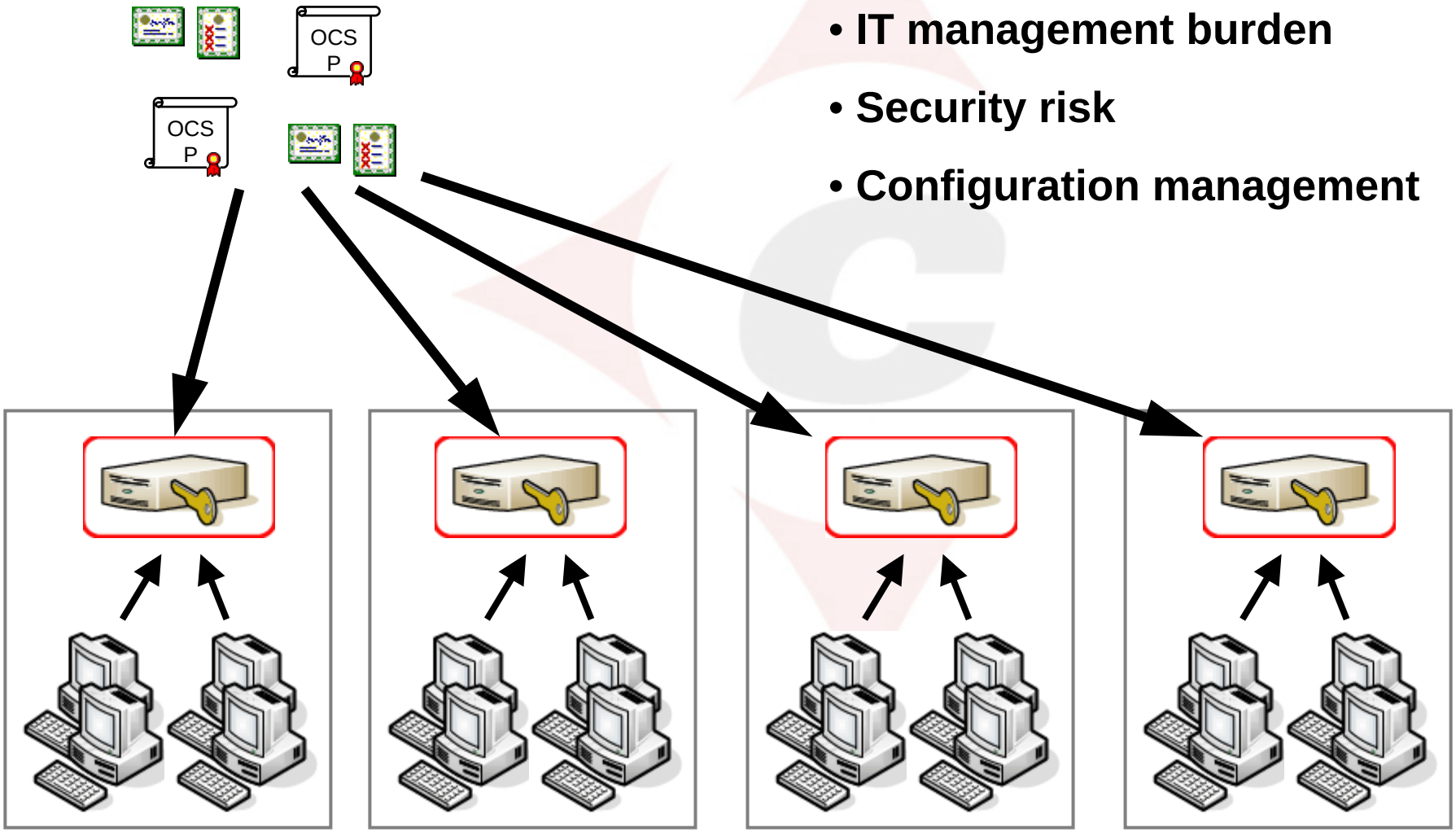


Option 1: DPV



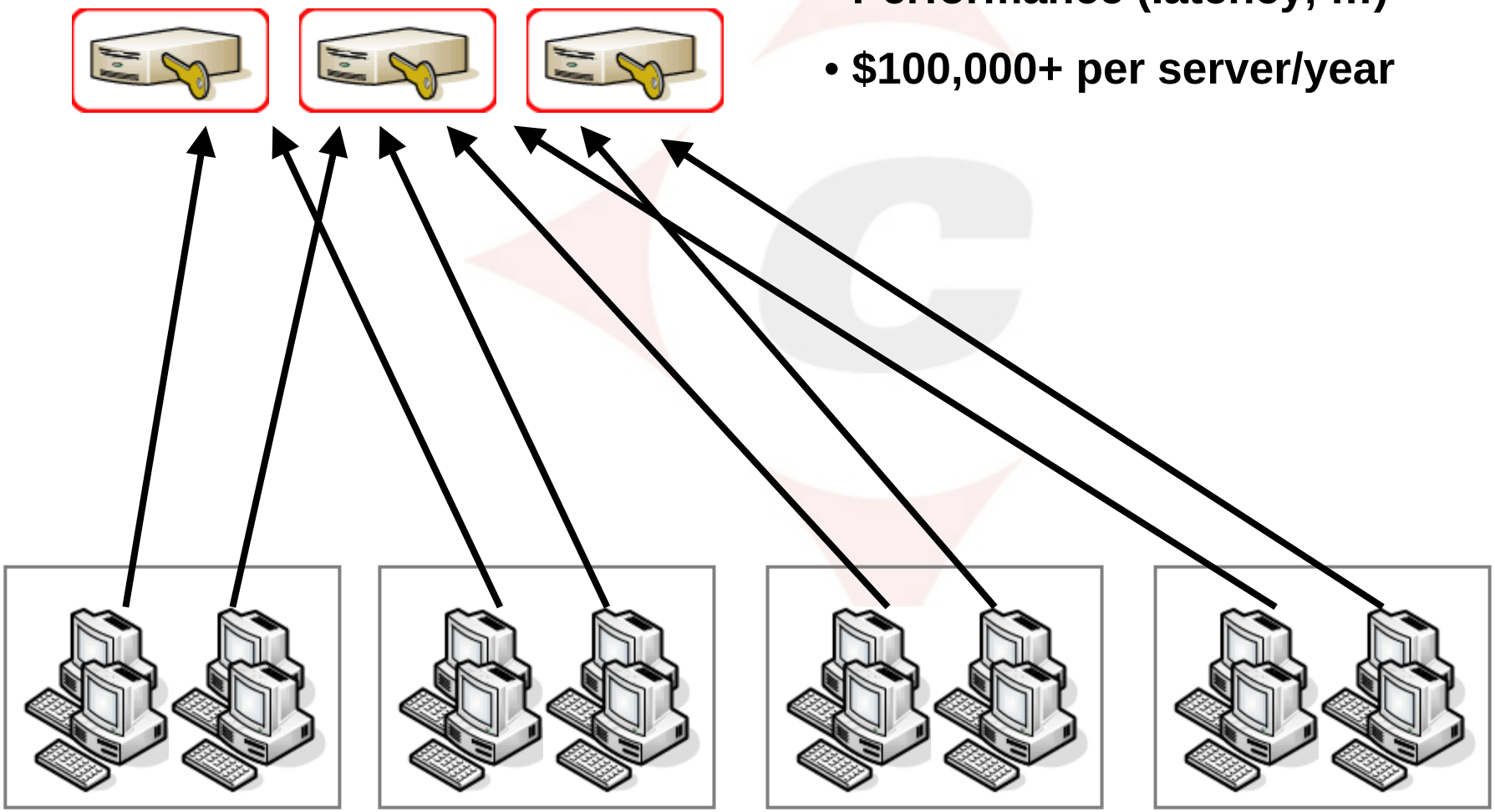
Local DPV Servers?

- High cost per server
- IT management burden
- Security risk
- Configuration management

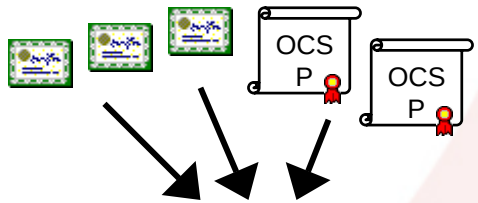


Central DPV servers?

- **Huge impact if compromised**
- **Performance (latency, …)**
- **$100,000+ per server/year**



Path Validation Option 2: DPD



CA certificates and OCSP responses

Lightweight server, no keys

"Can I trust this cert:

if I trust this root?"

State Dept. Root

Issuer: State Dept. Root
Subject: FBCA

FBCA: Good

Issuer: FBCA
Subject: DoD Root

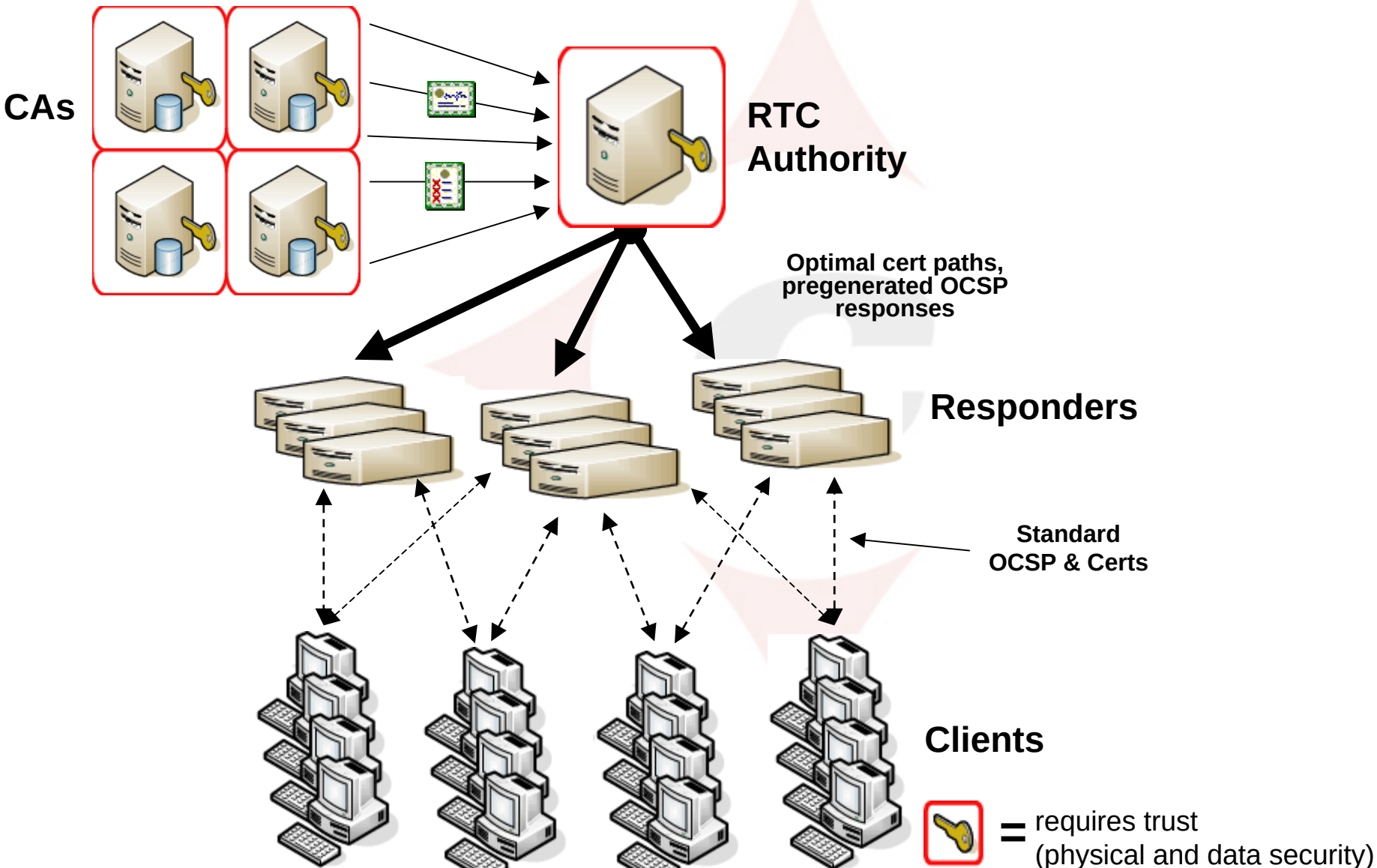
DoD Root: Good

Issuer: DoD Root
Subject: DoD CA-7

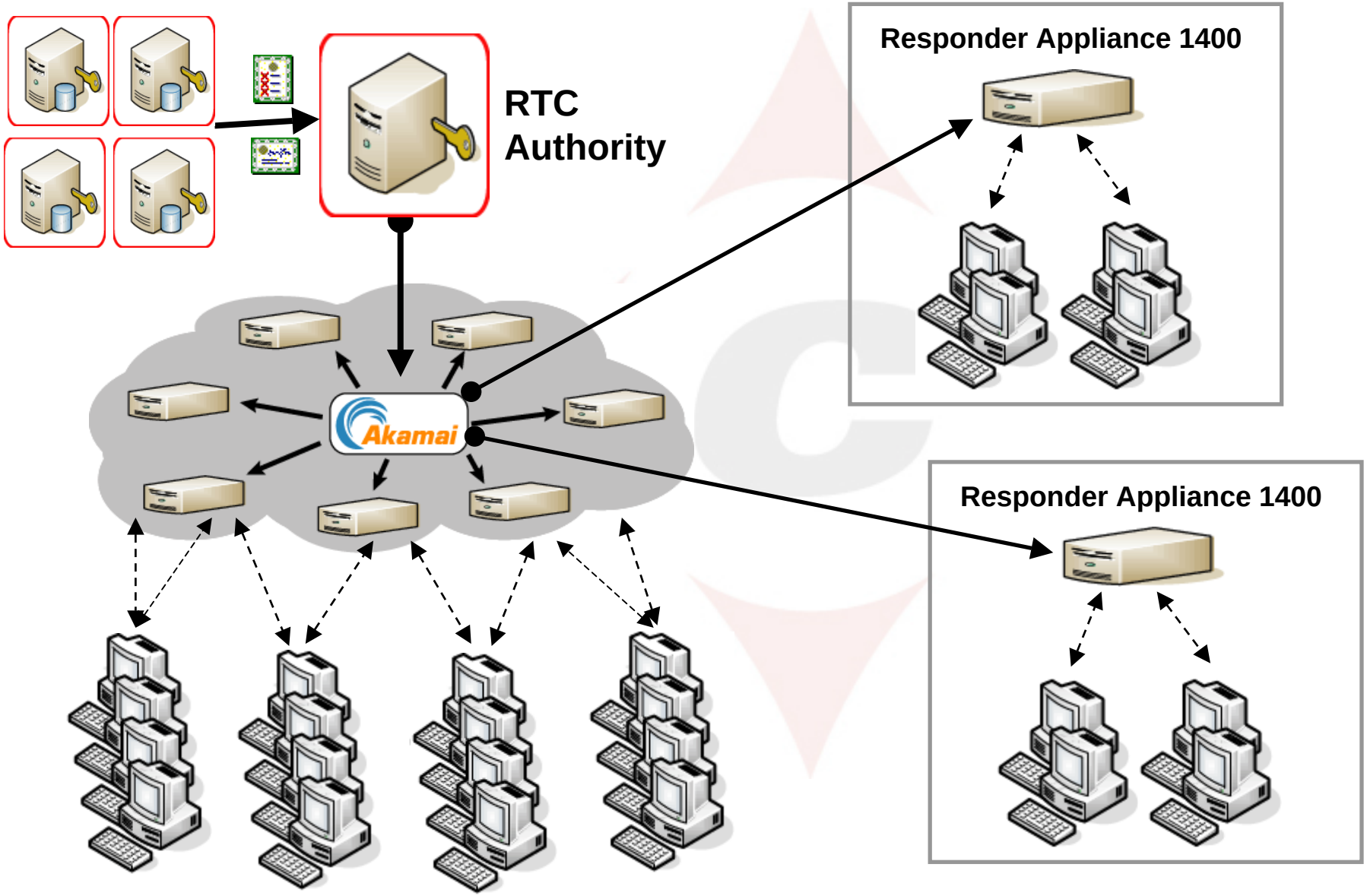
DoD CA-7: Good

D. Rumsfeld: Good

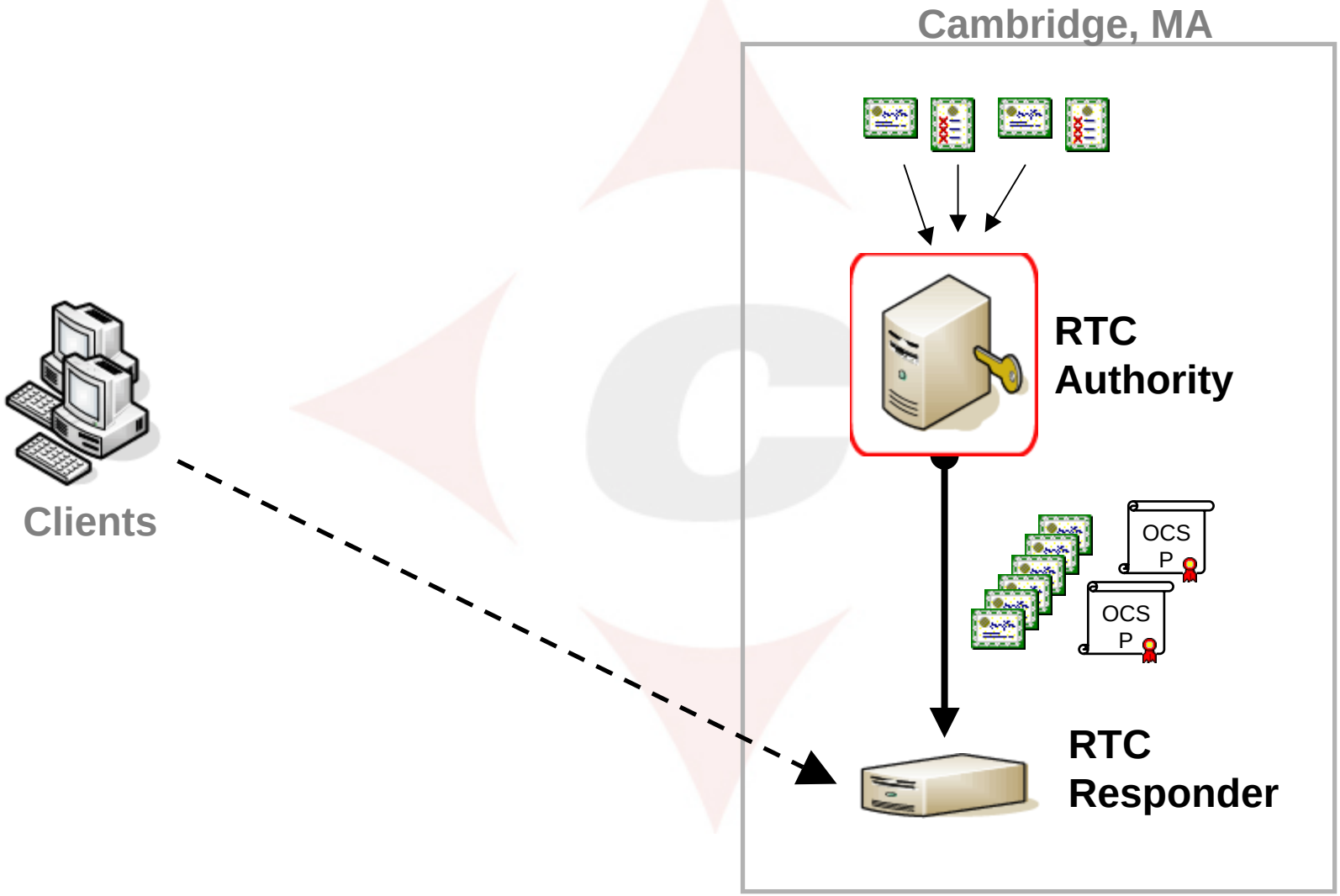
Distributed DPD



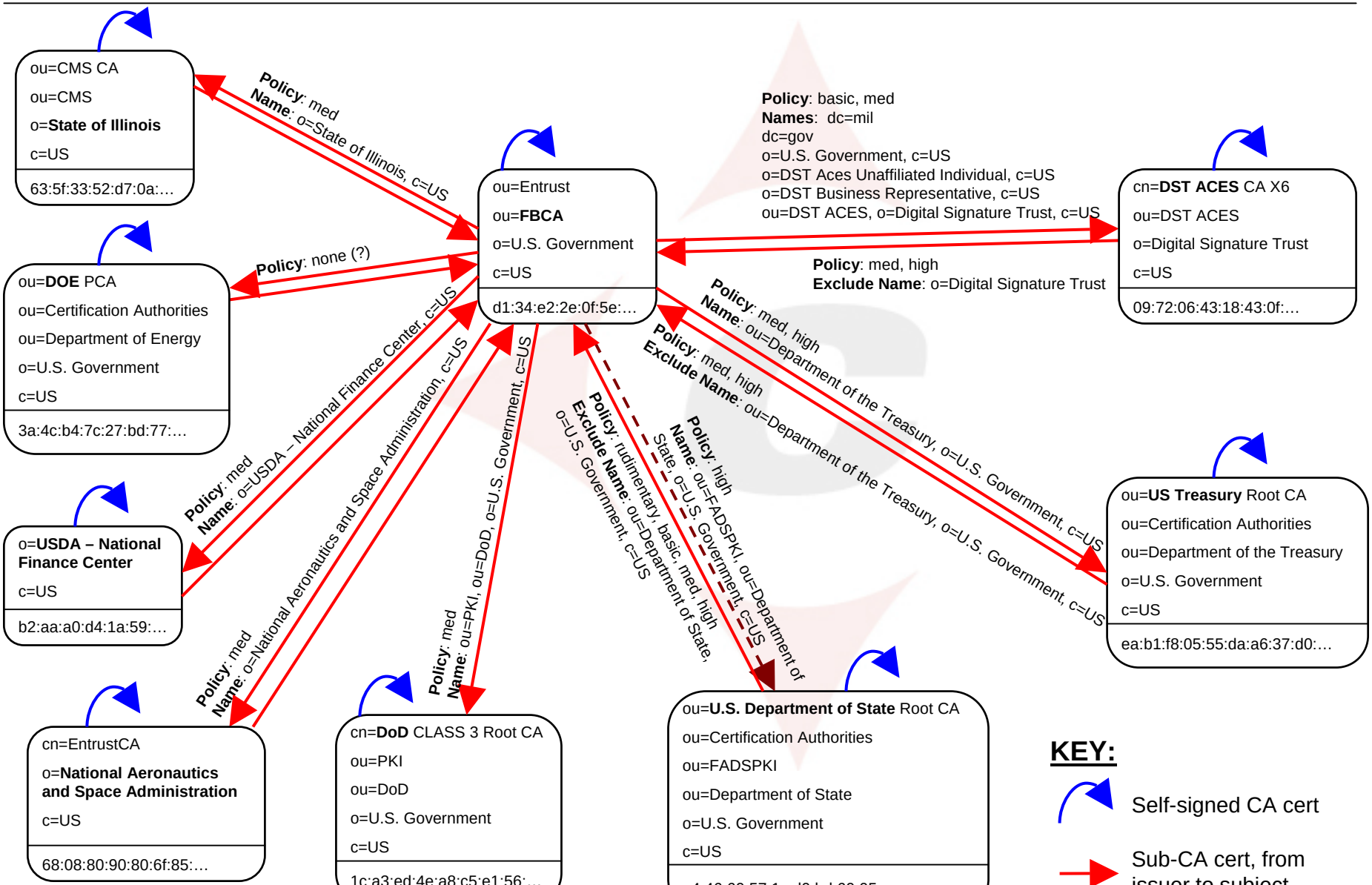
D-DPD: Managed, Hybrid Options



DPD Server Demonstration

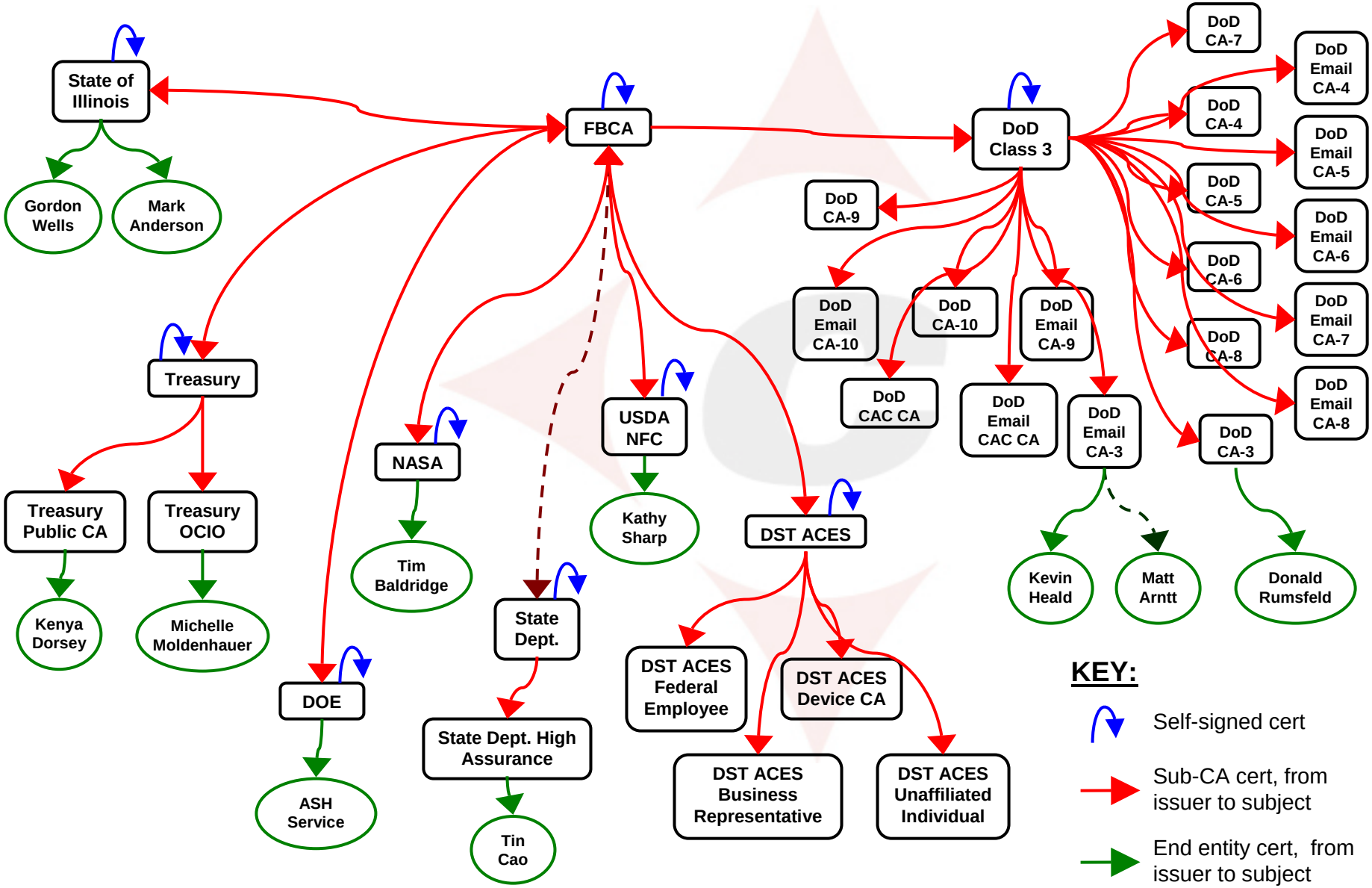


Federal Bridge CA



CoreStreet
REAL TIME CREDENTIALS

FBCA and Subordinates



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