



# CoreStreet's

# Distributed Certificate Validation

**Randy Bowman**  
**Principal Systems Engineer**  
**Corestreet Ltd. Federal Team**

**[rbowman@corestreet.com](mailto:rbowman@corestreet.com)**

***Cell: (301) 254-3858***

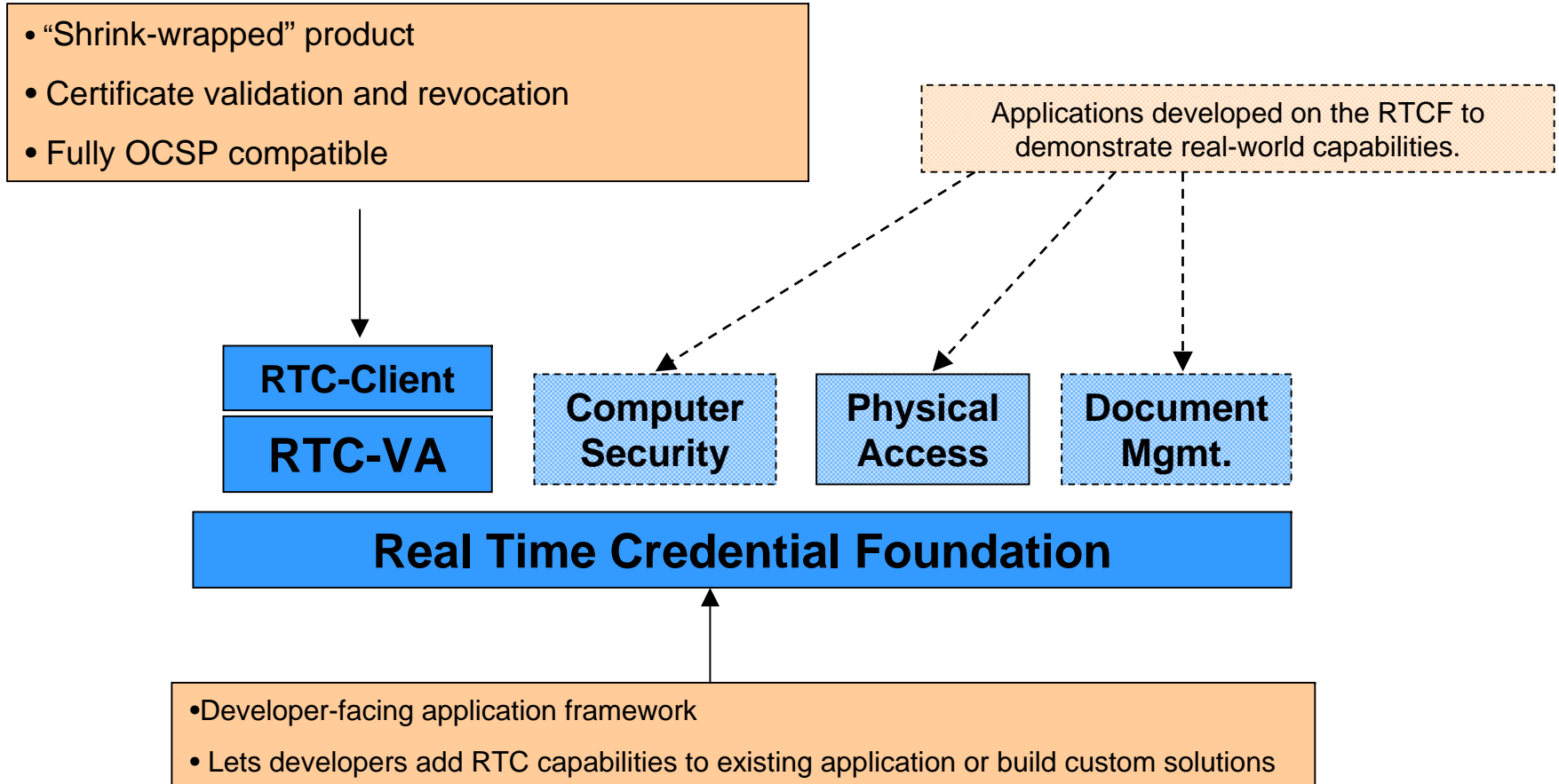
- **About CoreStreet**
- **CoreStreet Products and Services**
- **Technology Basics**
- **Distributed Certificate Validation**
- **DISA Validation System Facts & Readiness**
- **Vision**

# CoreStreet in a Nutshell

---

- What We Make: **Massively scalable software for validating people, documents, computers, devices, etc.**
- Founded: **October 2001**
- Employees: **35**
- Headquarters: **Cambridge, MA**
- IP: **16 issued patents + 18 filed patents**
- Target Markets: **Government, financial services, healthcare sectors.**
- Customers: **Identrus, three major federal agencies, two Global 1000 companies**
- Funding: **Privately funded**

# Our Products



# First Some Definitions

---

- **Identity** “the qualities of a person that make them different”
  - Name, age, date of birth, physical features
- **Authentication** is proving your claimed identity
  - The picture on your driver’s license
- **Authorization** is granting privileges (process)
  - Privilege to drive, pass to enter military base
- **Credentials** are “evidence of one’s relationship or privileges”
  - Driver’s license represent relationship with state that issued it
- **Validation** is verifying your credentials are in good standing
  - Your relationship to the credentialing authority is still in good standing
  - Your privilege to drive has not been revoked

# It's a 2 Step Process!

---

**Today, more than ever, there is a critical need to:**

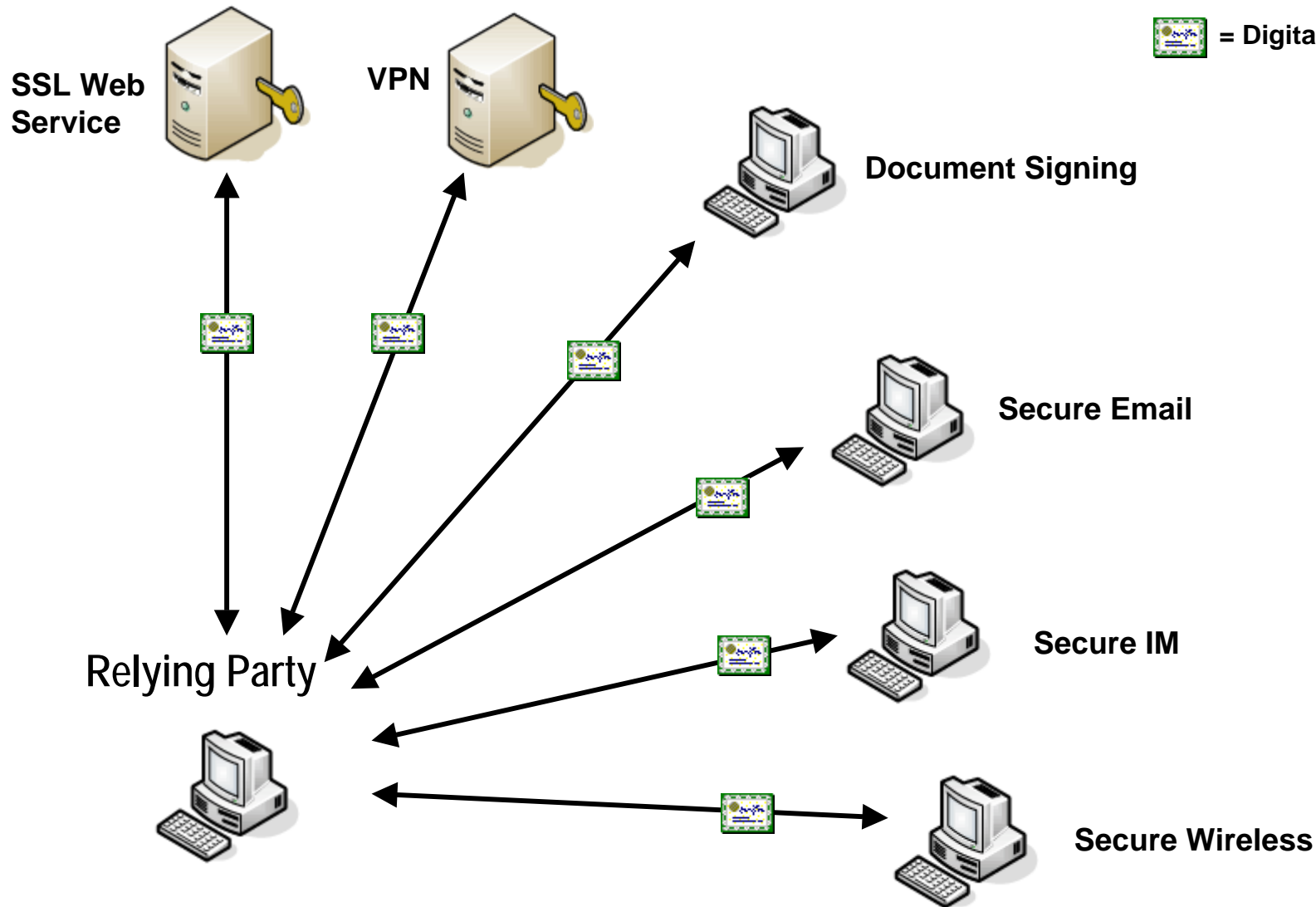
- Positively identify people, and then
- Decide if they should be allowed access to a place, device or function

**Secure access therefore reduces to answering two critical questions:**

1. Are you who you say you are? (*Authentication*)
2. Are you suppose to be doing what you are trying to do, right now? (*Validation*)

# Certificate Validation Examples

 = Digital Certificate



- **Certificate Revocation Lists (CRLs)**
  - Traditional CRLs
  - MiniCRLs
- **Online Certificate Status Protocol (OCSP)**
  - Traditional OCSP
  - Distributed OCSP

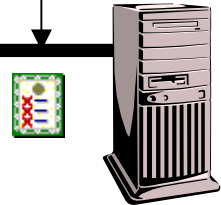


# CRL

**Certificate Authority**

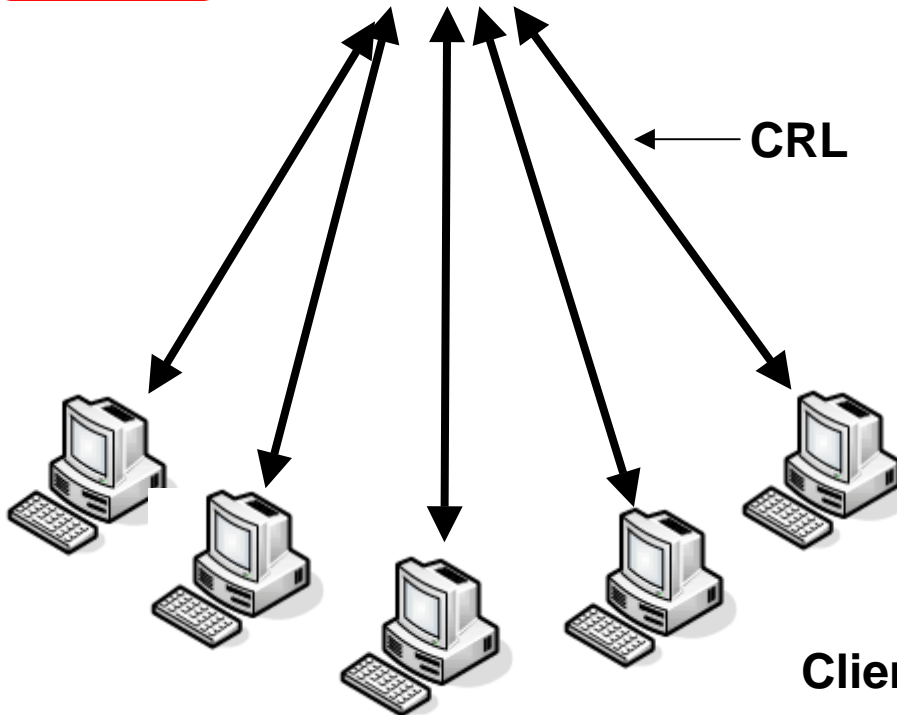


CRLs



**Directory Server**

CRL



**Clients**

## Advantages

- Easy to manage for small numbers
- Works with all issued certificates
- Industry standard

## Disadvantages

- Large bandwidth to the clients
- Does not scale



= requires trust  
(physical and data security)

# CRL Problem #1: Scalability

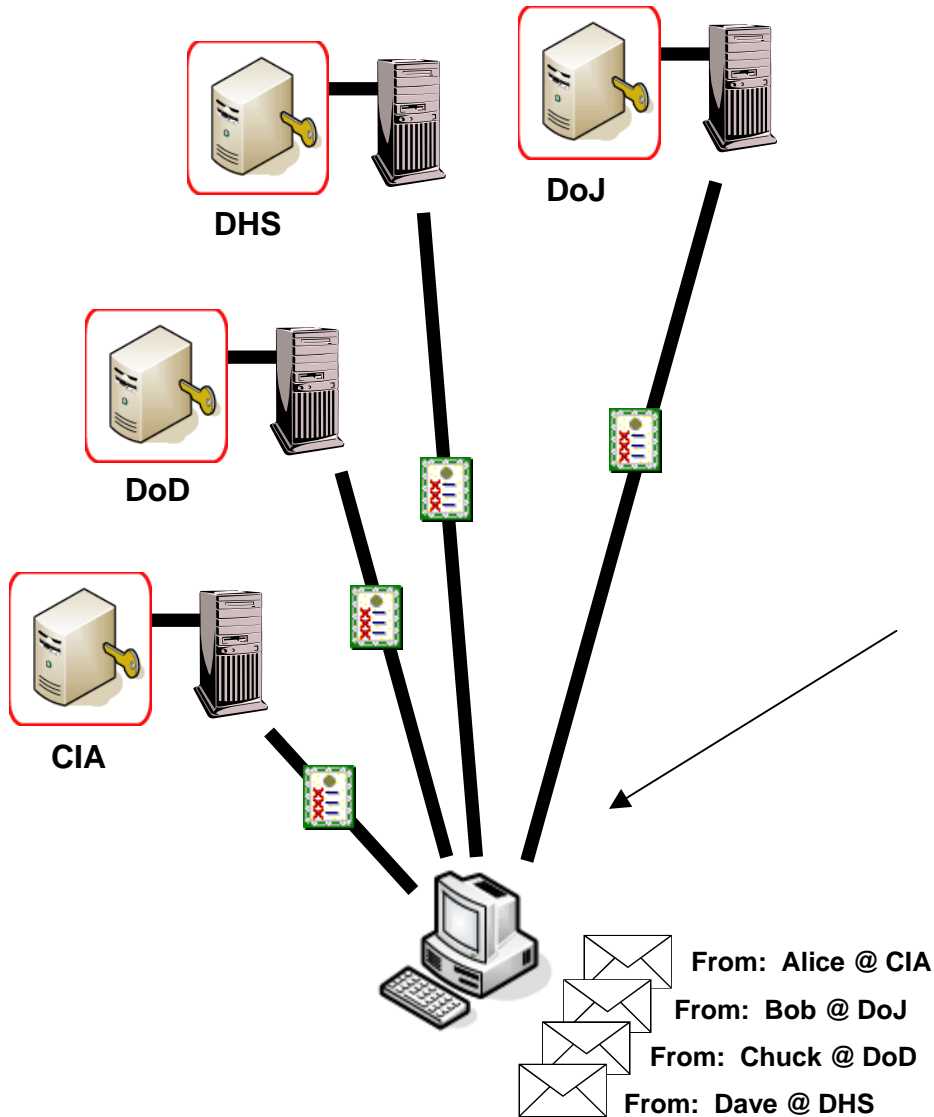
---

- **CRLs grow to unmanageable sizes**
  - DoD CRLs already at 2-7 Megabytes Each (nearly 40MB)
  - Download times of 7-14 minutes
  - Current 17% revocation rate expected to grow
- **CRLs need to be distributed to every relying party application**
  - All data goes to all applications

**Bottom line:**

## **CRLs Do Not Scale!**

# CRL Problem #2: Performance



**Need CRLs for all  
accepted certificates:**

**Federation explodes  
performance problem**

## 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

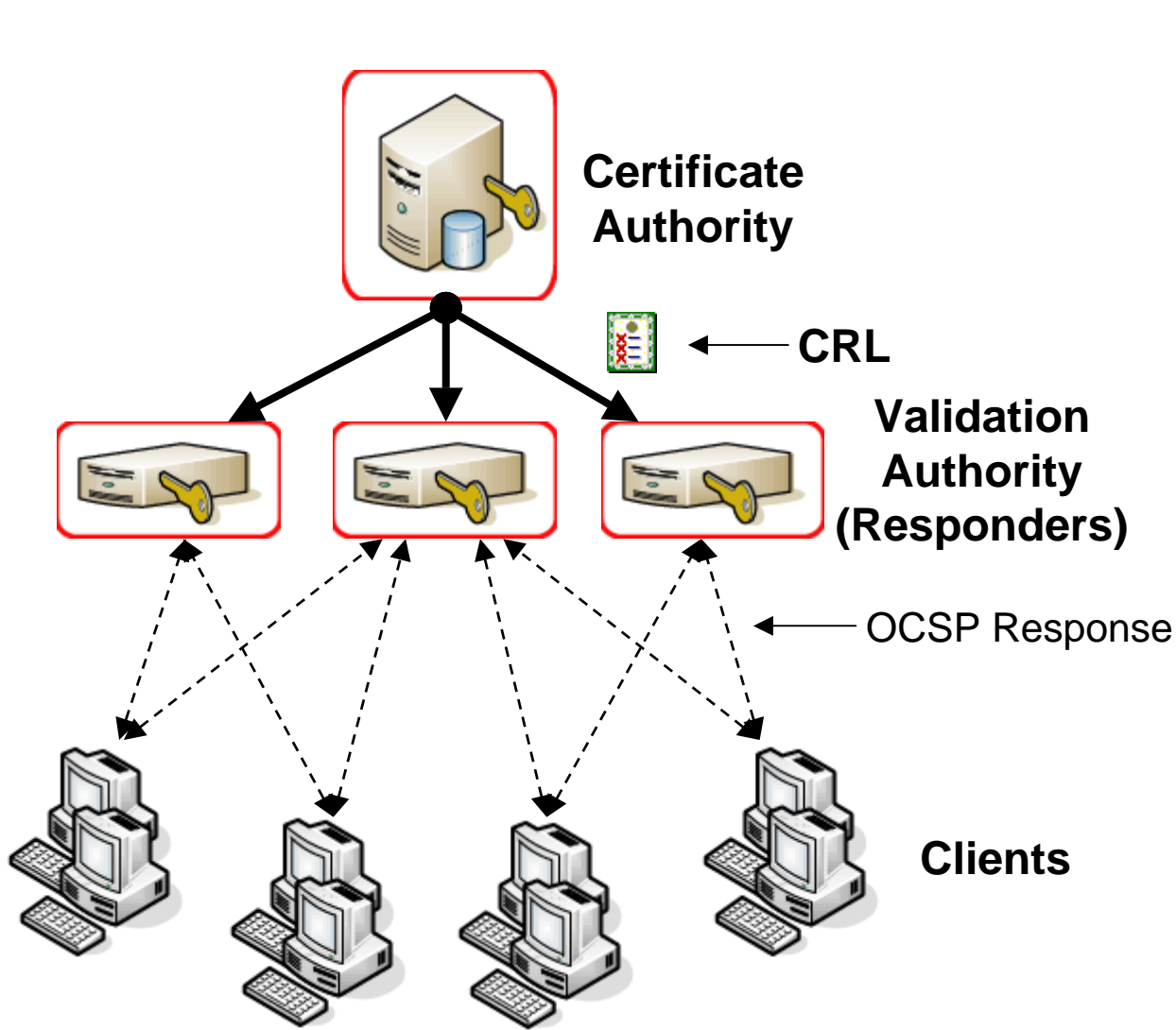
## OCSP libraries/plug-ins:

- 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)

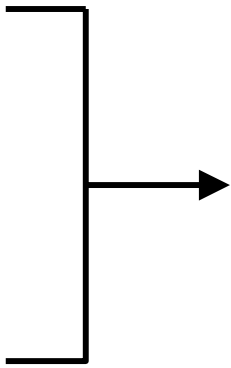
# Traditional OCSP



Advantages
<ul style="list-style-type: none"> <li>• Small bandwidth to clients</li> <li>• Works with issued certificates</li> <li>• Industry standard</li> </ul>
Disadvantages
<ul style="list-style-type: none"> <li>• Requires secured responders</li> <li>• Expensive to scale</li> <li>• Slow response time to client</li> <li>• Single point of failure</li> <li>• Failover issues</li> </ul>

 = requires trust (physical and data security)

- **How many OCSP responders to deploy?**
  - Cost issue
- **Where to put the OCSP responders?**
  - Cost and security issue
- **How to use OCSP in tactical environments?**
  - Security and rapid response issue
- **How does a relying party application trust the response it receives from an OCSP responder?**
  - Security and operational issue

- High Performance
  - High Availability
  - Truly Scalable
  - Secure
  - Cost effective
- 
- Distributed Validation**  
Numerous, local responders

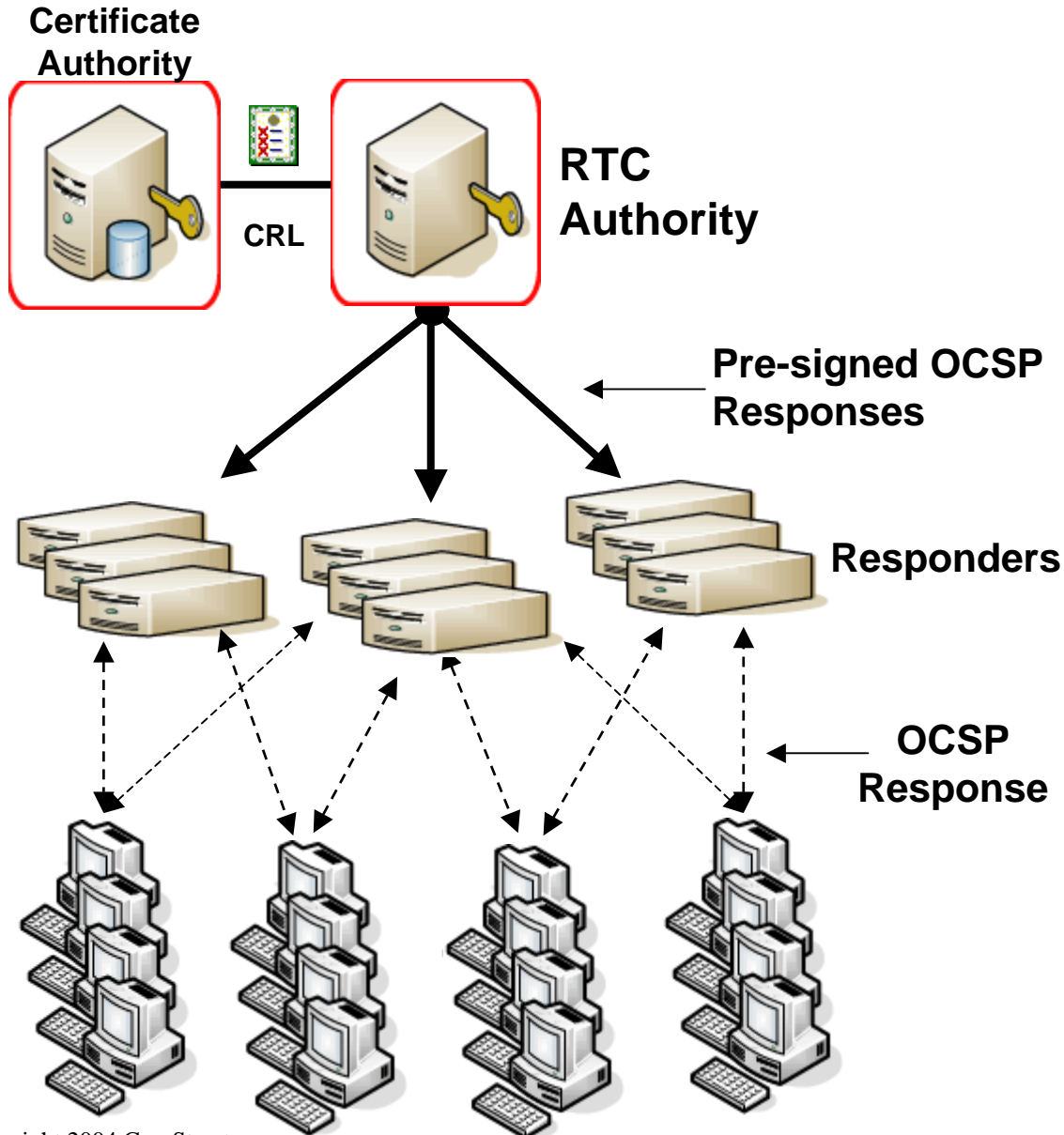
**How to provide Distributed Validation that is cost effective and secure?**

## Design Principle


*Separate the security sensitive data and trusted operations from the **delivery process** of providing certificate status to relying party applications.*



# Distributed OCSP

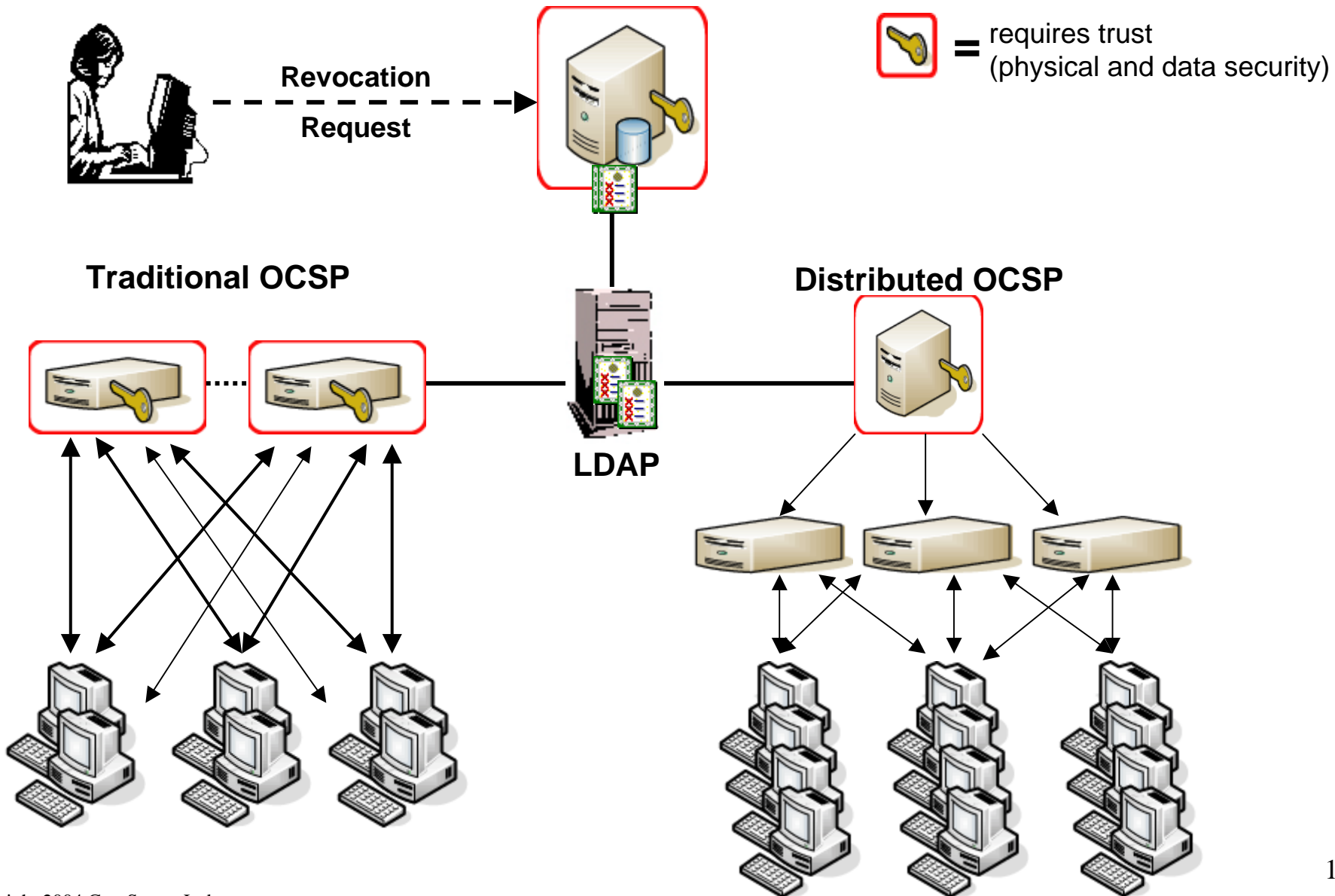


- | Advantages                        |
|-----------------------------------|
| • Uses unsecured responders       |
| • Cost Effective                  |
| • Small bandwidth to clients      |
| • Response 20X faster than T-OCSP |
| • Works with issued certificates  |
| • Industry standard               |
| • Scales to 10s millions of users |
| • No impact to client apps        |
| • No impact to CA infrastructure  |
| • Single key to manage            |
| • Inherently more secure          |

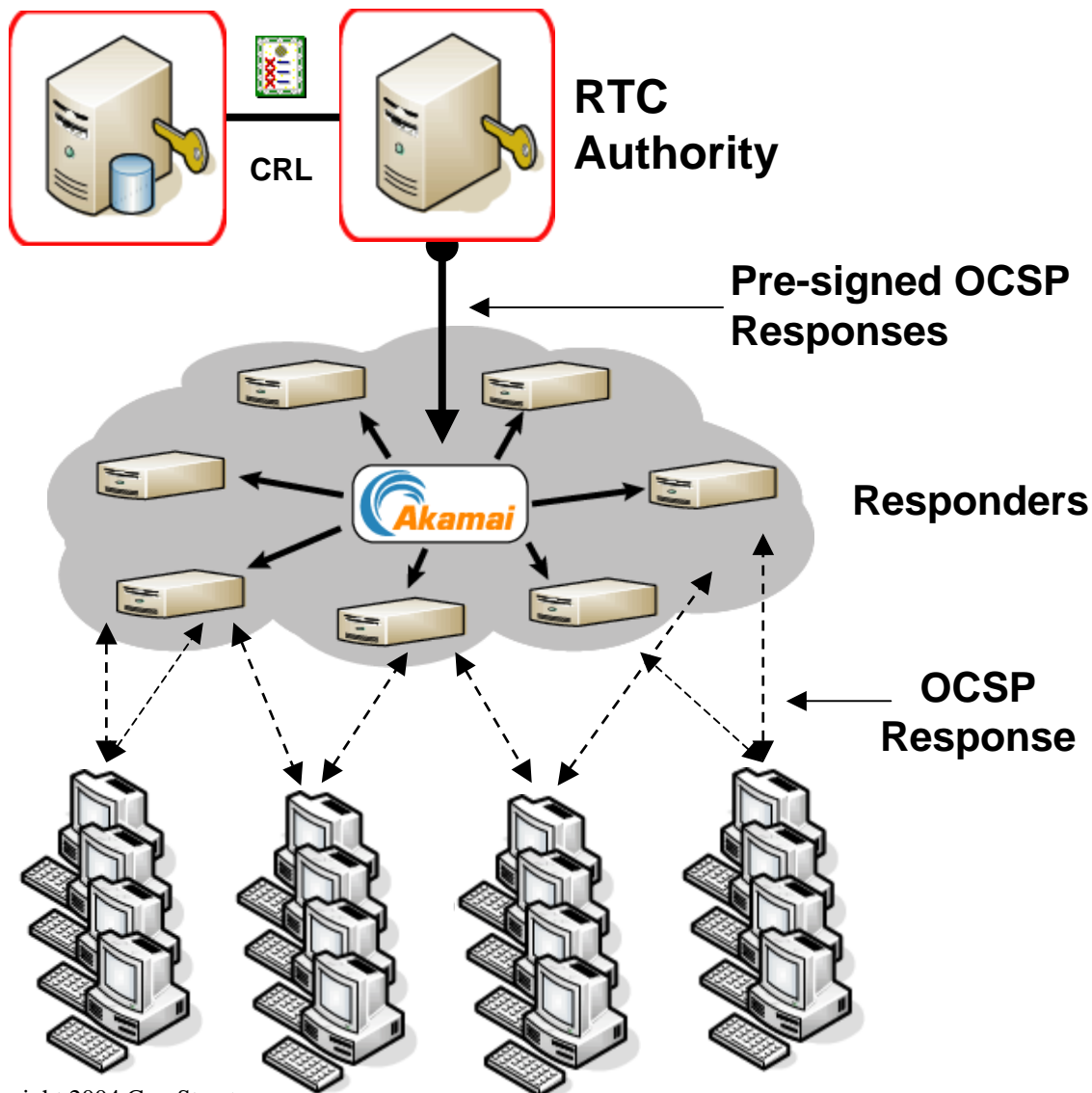
 = requires trust (physical and data security)

- **How many OCSP responders to deploy?**
  - As many as needed
- **Where to put the OCSP responders?**
  - Close to users
- **How to use OCSP in tactical environments?**
  - Set up responder, provide connectivity
- **How does a relying party application trust the response it receives from an OCSP responder?**
  - Short-lived certs from one Validation Authority

# True Scalability



# Distributed OCSP, Managed



## DISA Validation System Facts

- Live on October 16, 2003
- # Certs supported > 12 million
- # CAs/CRLs supported = 19 + 1
- # Responders = 20
- # Global sites = 10
- Ave response time = 65 milliseconds
- Responder capacity > 1,000 r/sec
- System accessed by users from:
  - 8 foreign countries
  - 19 different states



= requires trust  
(physical and data security) 20

# Valid Response

CoreStreet Validation Demo


**CoreStreet Validation**


The Certificate for:

CHRISTINE BOWMAN

has been Validated and is:

**Good**

 Time to Validate: **0.431 seconds**

 **Details** Issued By: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DOD CLASS 3 EMAIL CA-5

Certificate		CRL	Contact
Serial Number		Revocation Reason	Email
0x74D5E		Not Revoked	christine.bowman@langley.af.mil
Issued	Expires	Freshness	<input checked="" type="checkbox"/> Send Whitepaper <input type="button" value="Contact Me"/>
10/22/2003	10/21/2006	10 Hours, 13 Minutes, 17 Seconds	

# Revoked Response

CoreStreet Validation Demo


**CoreStreet Validation**

The Certificate for:


Matthew Arntt

has been Validated and is:

**Revoked**

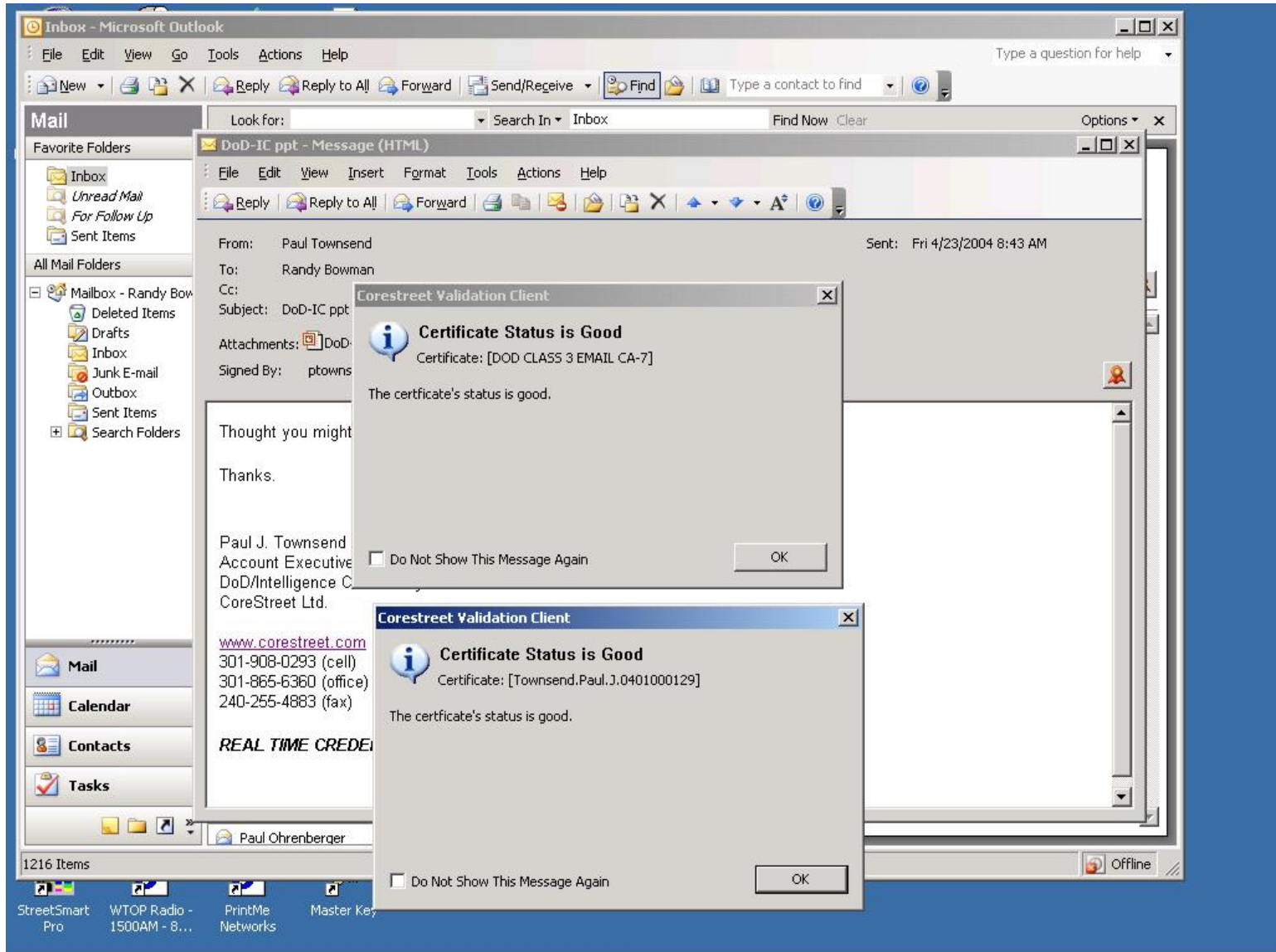
 Time to Validate: 0.43 seconds

---

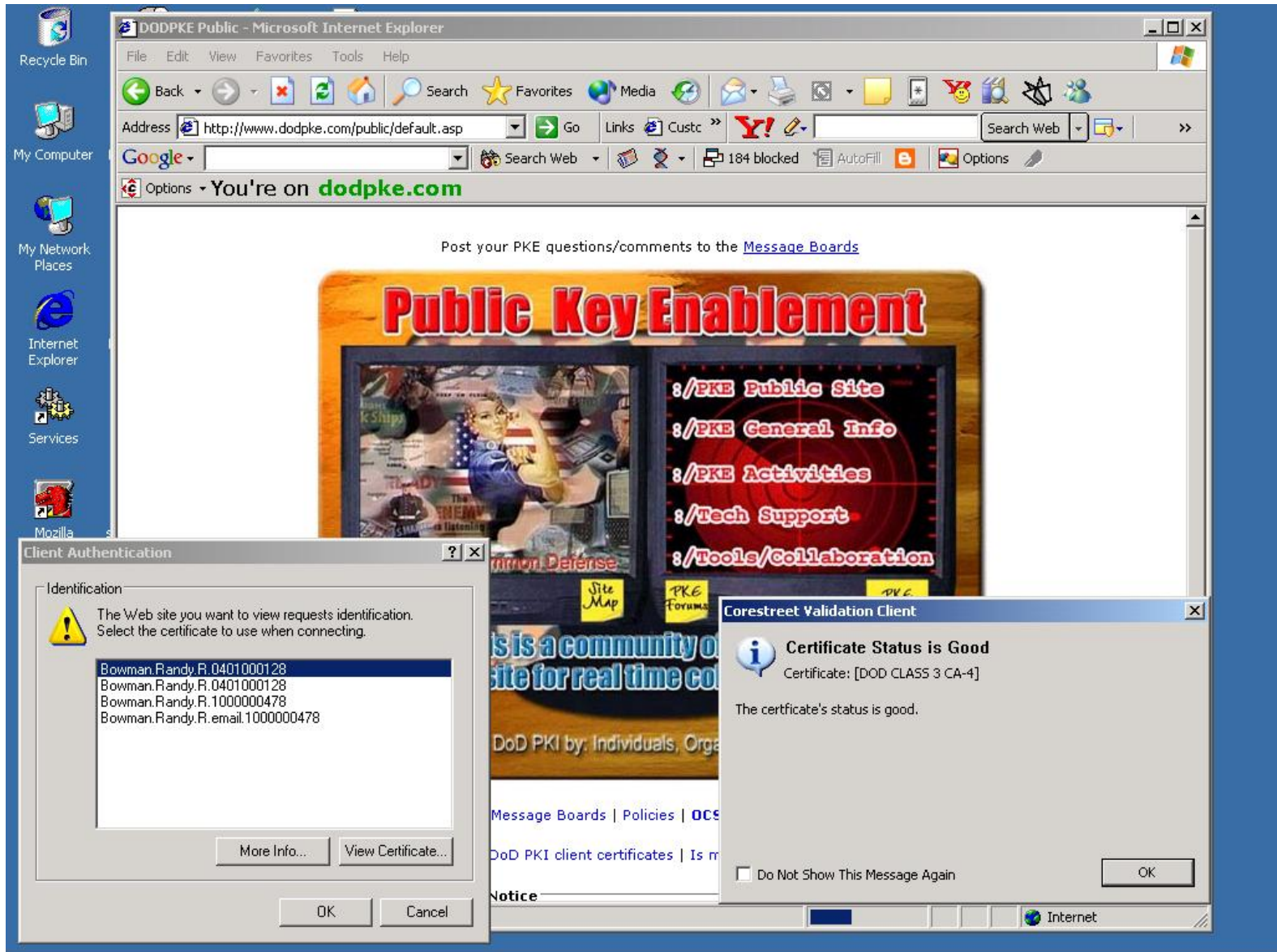
 **Details** Issued By: C=US, O=U.S. Government, OU=DoD, OU=PKI, CN=DOD CLASS 3 EMAIL CA-3

Certificate		CRL	Contact
Serial Number		Revocation Reason	Email
0x49B3D		Unspecified	matt_arntt@sra.com
Issued	Expires	Freshness	<input checked="" type="checkbox"/> Send Whitepaper <input type="button" value="Contact Me"/>
7/10/2002	7/10/2005	16 Hours, 39 Minutes, 55 Seconds	

# Signed Email Checks Signer and CA



# Web Server Certs Validated



The screenshot shows a Windows desktop environment. In the background, a Microsoft Internet Explorer window is open to the URL <http://www.dodpke.com/public/default.asp>. The browser's address bar shows the address and navigation buttons. The main content area of the browser displays a webpage titled "Public Key Enablement" with a navigation menu listing links such as "/PKE Public Site", "/PKE General Info", "/PKE Activities", "/Tech Support", and "/Tools/Collaboration".

In the foreground, two dialog boxes are open. The "Client Authentication" dialog box is on the left, displaying a warning icon and the text: "The Web site you want to view requests identification. Select the certificate to use when connecting." Below this text is a list of certificates:

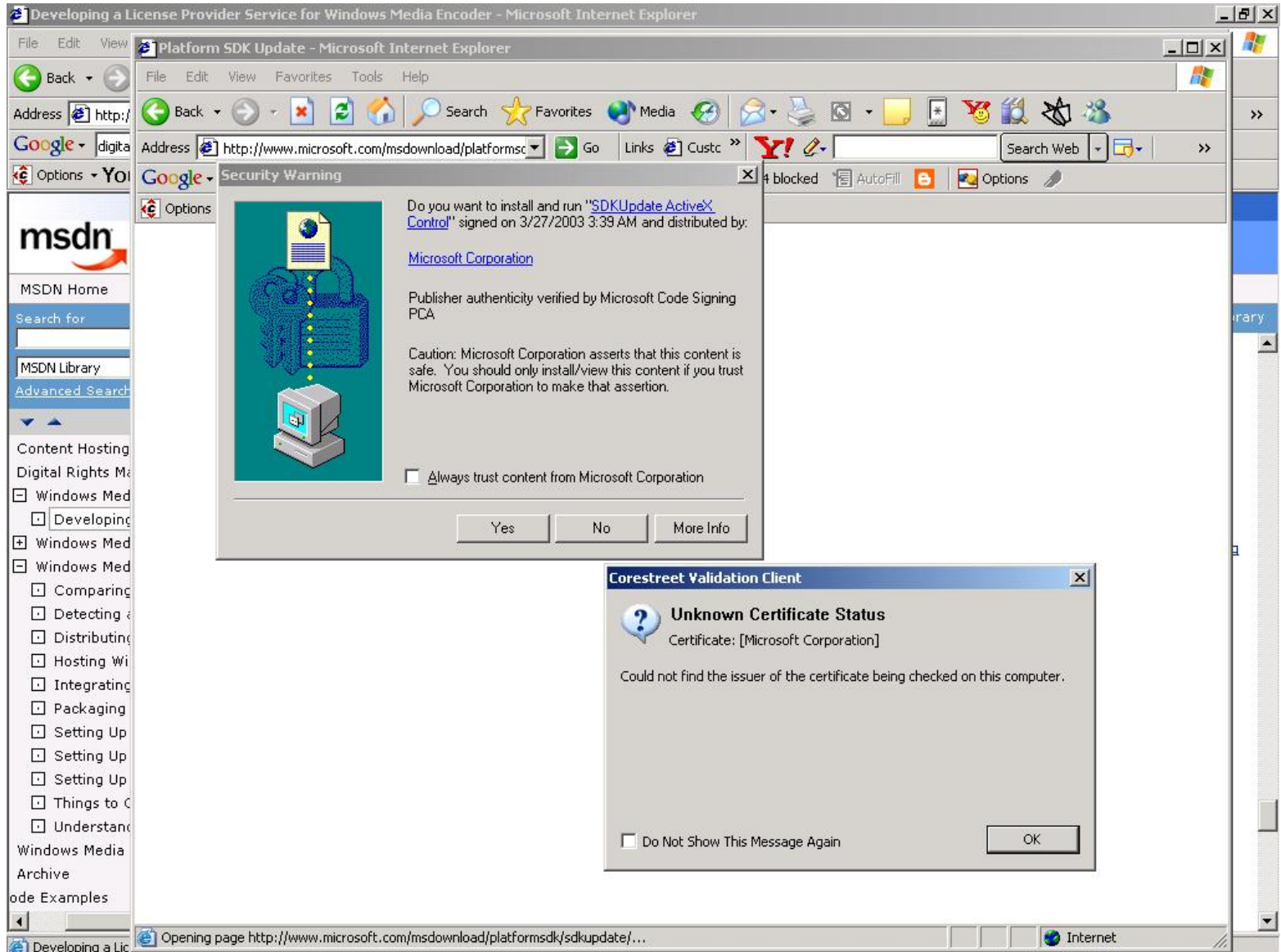
- Bowman.Randy.R.0401000128
- Bowman.Randy.R.0401000128
- Bowman.Randy.R.1000000478
- Bowman.Randy.R.email.1000000478

Buttons for "More Info...", "View Certificate...", "OK", and "Cancel" are visible at the bottom of the dialog.

The "Corestreet Validation Client" dialog box is on the right, displaying an information icon and the text: "Certificate Status is Good" and "Certificate: [DOD CLASS 3 CA-4]". Below this, it states: "The certificate's status is good." There is a checkbox for "Do Not Show This Message Again" and an "OK" button at the bottom right.



# Code Signing w/ Status Unknown

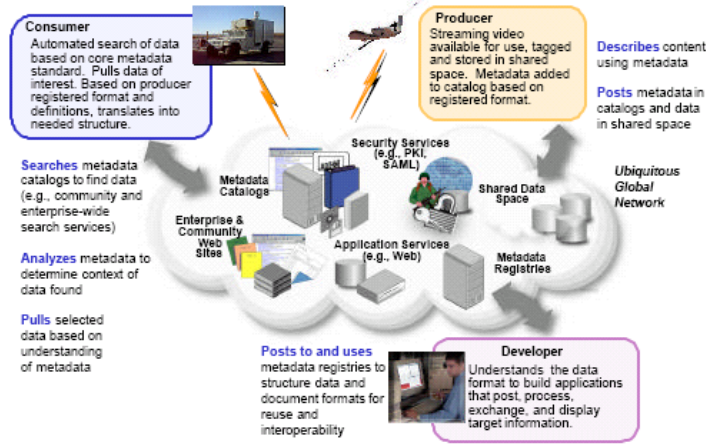
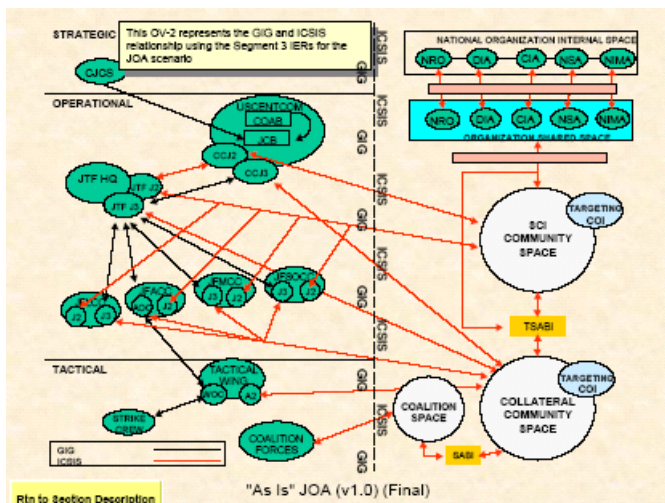
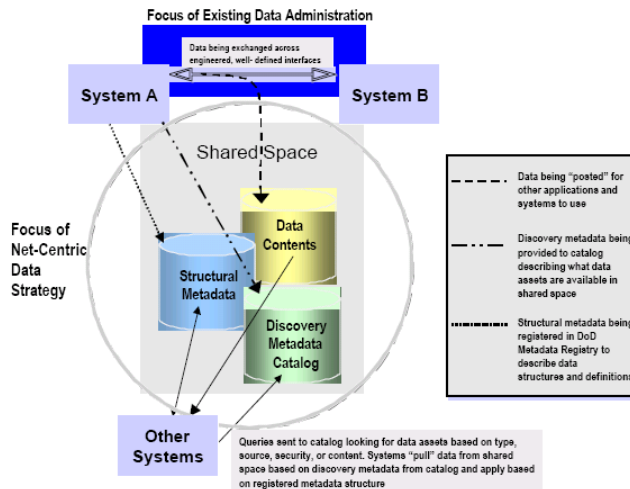


- **Performance**
  - Operational correctness, response time, data “freshness”
- **Availability**
  - 100% up time (improved SLA), successful upgrades, global users
- **Scalability**
  - 20 CAs, 12 million certs, > 1,000 rqst/sec/responder , ECA added
- **Security**
  - Secure against Intrusion, DoS, Replay attacks, in NIAP evaluation
- **Interoperability**
  - JITC certified, work with multiple CAs, clients, applications
- **Cost effectiveness**
  - Infrastructure cost savings versus traditional OCSP > 70%

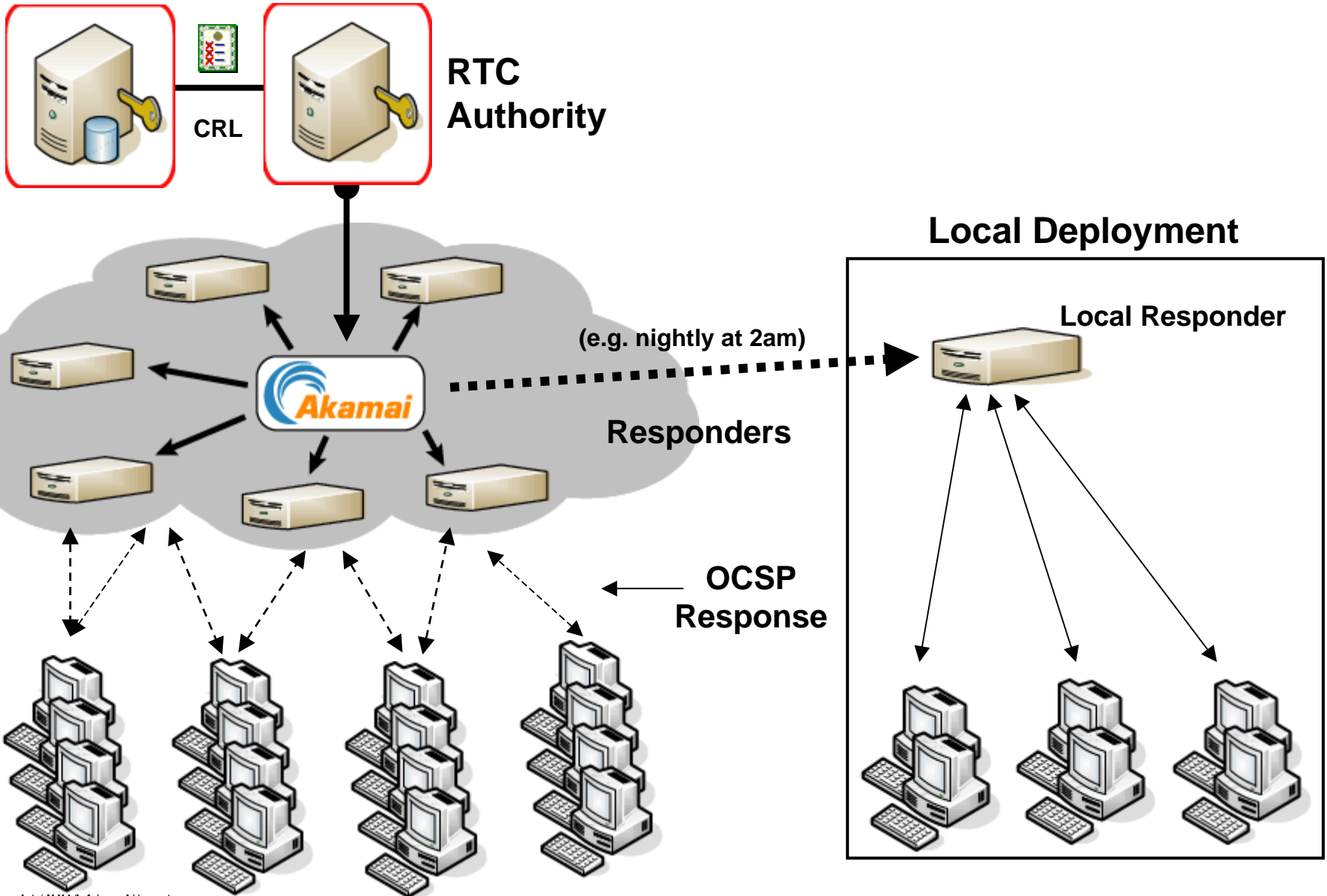
- **Questions about Today?**
- **Let's Share the Vision!**

[rbowman@corestreet.com](mailto:rbowman@corestreet.com)

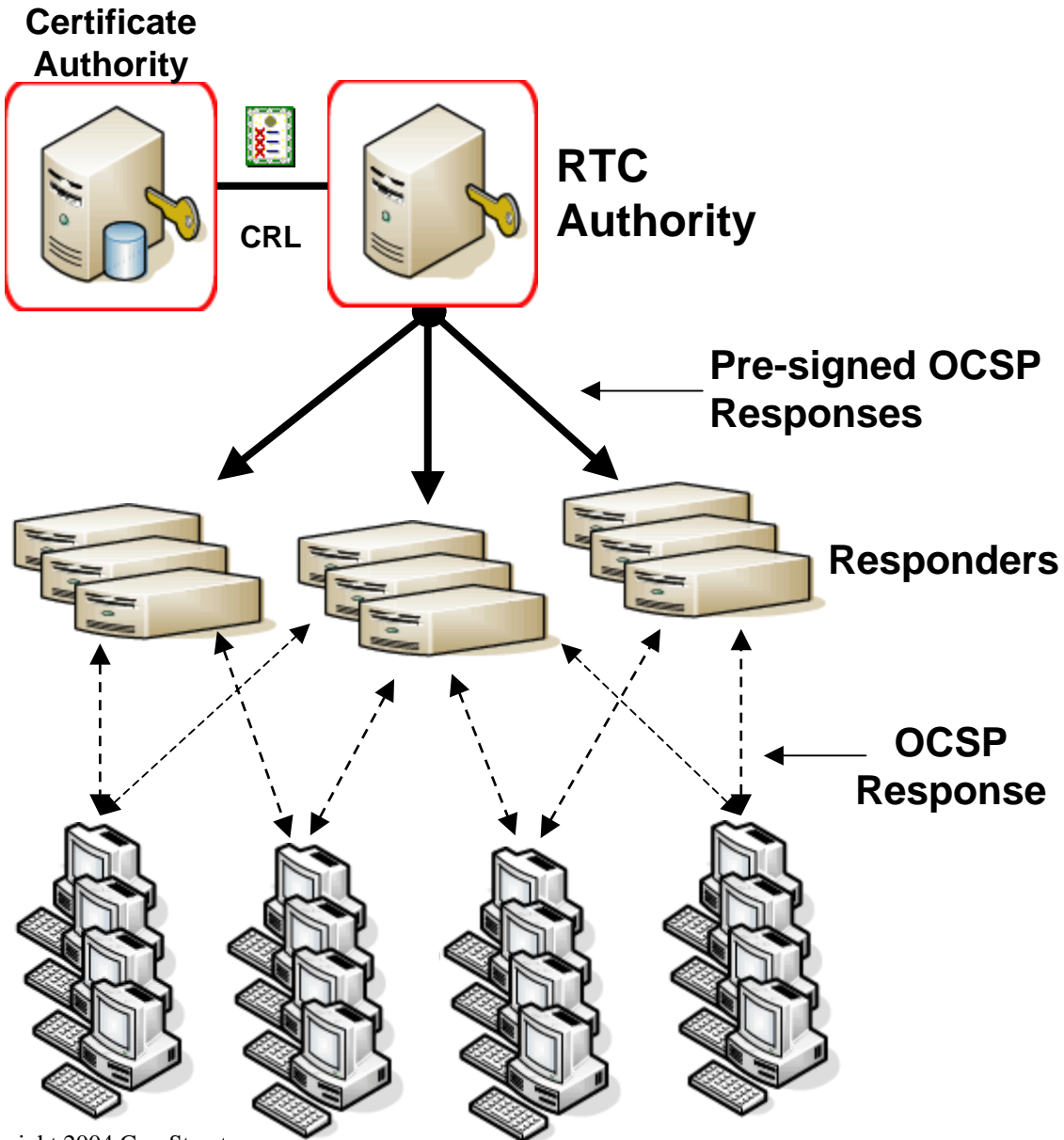
# NCES Sharing Data



# Distributed OCSP, Mixed



# Distributed OCSP with Privileges



**OCSP Response**  
Certificate #1234:

- Is a Pilot
- Is not an Inspector

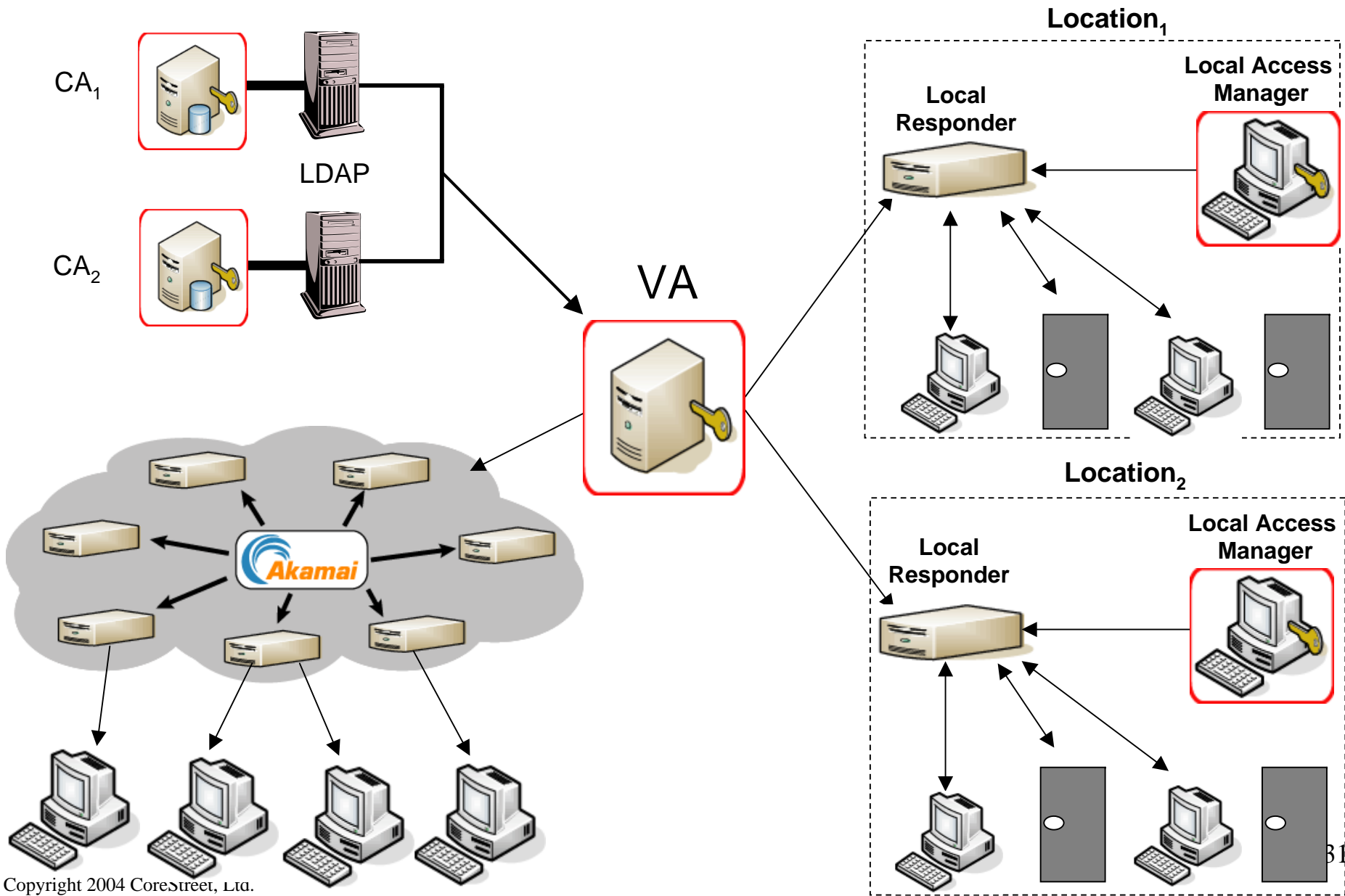
Signed:  
RTC Authority

TSA

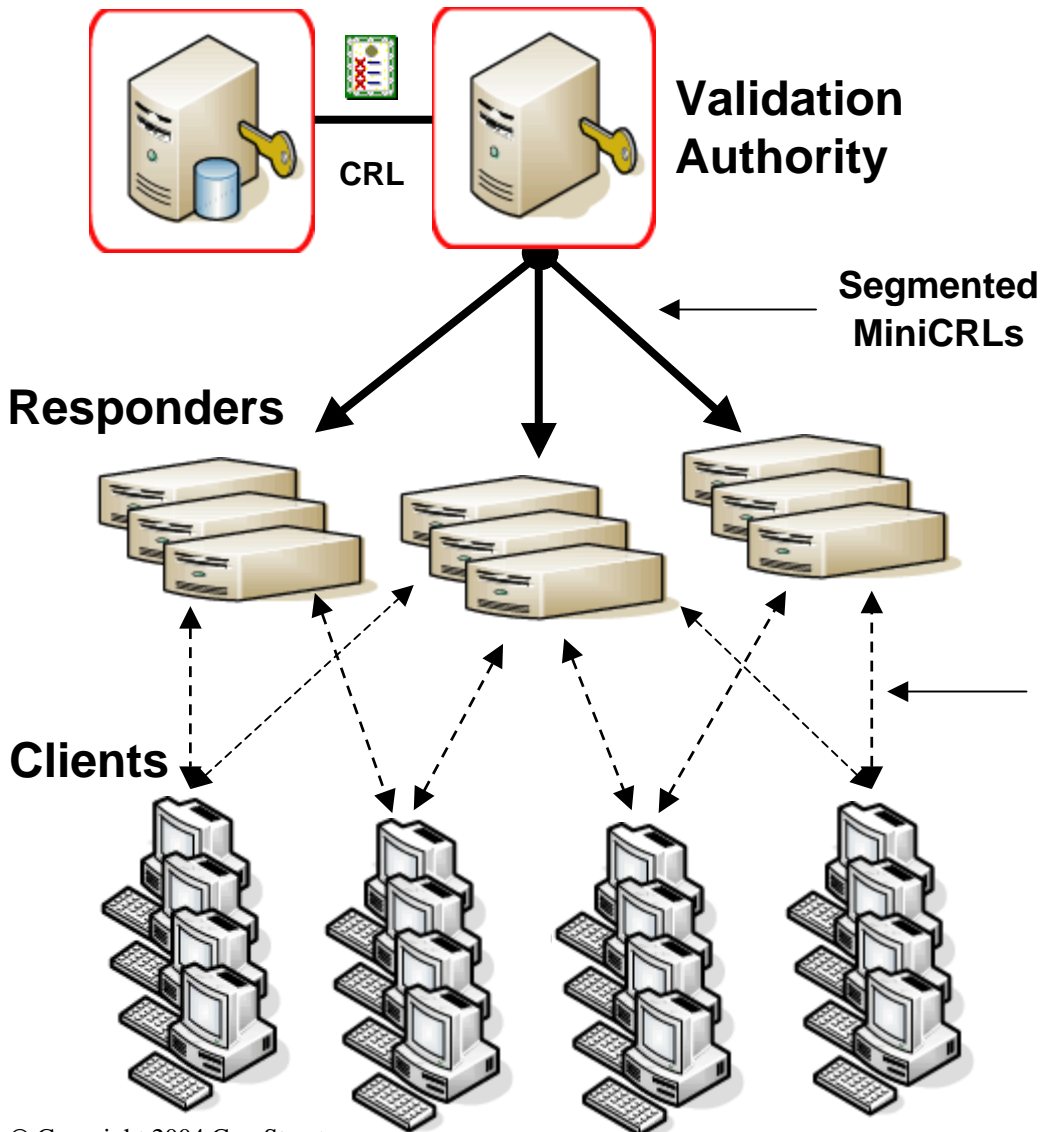
James M. Loy

= requires trust (physical and data security) 30

# Merging Physical and Logical Access



# MiniCRL



**How It Works**

- VA sends a segmented and highly compressed (30X average) CRL to each responder.
- Responder sends individual segments to client.

**Advantages**

- Smallest bandwidth between VA and responders
- Small bandwidth between responder and clients
- No trusted responders required
- Scales to 100s of millions of users
- Computationally simple (no signing per transaction)
- Works with all issued certificates

MiniCRL Segment

**Disadvantages**

- Not yet adopted as an industry standard
- New client plug-in required

= requires trust (physical and data security) 32