NIST PKI Implementation Workshop

Bob Dulude
Chief Security Officer

Agenda

- **CoreStreet support of HSPD-12 requirements**
  - OCSP validation requirement
  - Single credential for logical and physical access control
- **Validation requirements to consider**
  - Lessons learned from DoD deployment
- **Capturing the <u>benefits</u> of HSPD-12**
  - Using a ubiquitous, interoperable credential

CoreStreet

Life After Issuance

The success or failure of your PIV card deployment will rest with the end user's experience

***Validation** will play a key role in the user's **everyday** experience*

Validation Considerations #1

DoD’s main lesson learned

- CRLs do not scale, total size now over 100 MB
- Results in poor performance
- Not always available
- Issues will increase in federated environment
- Won’t be interoperable with mobile devices
  - Phones, PDAs, Blackberrys

CoreStreet

Validation Solution Criteria

- High Performance
- High Availability
- Truly Scalable
- Secure
- Interoperable
- Cost effective

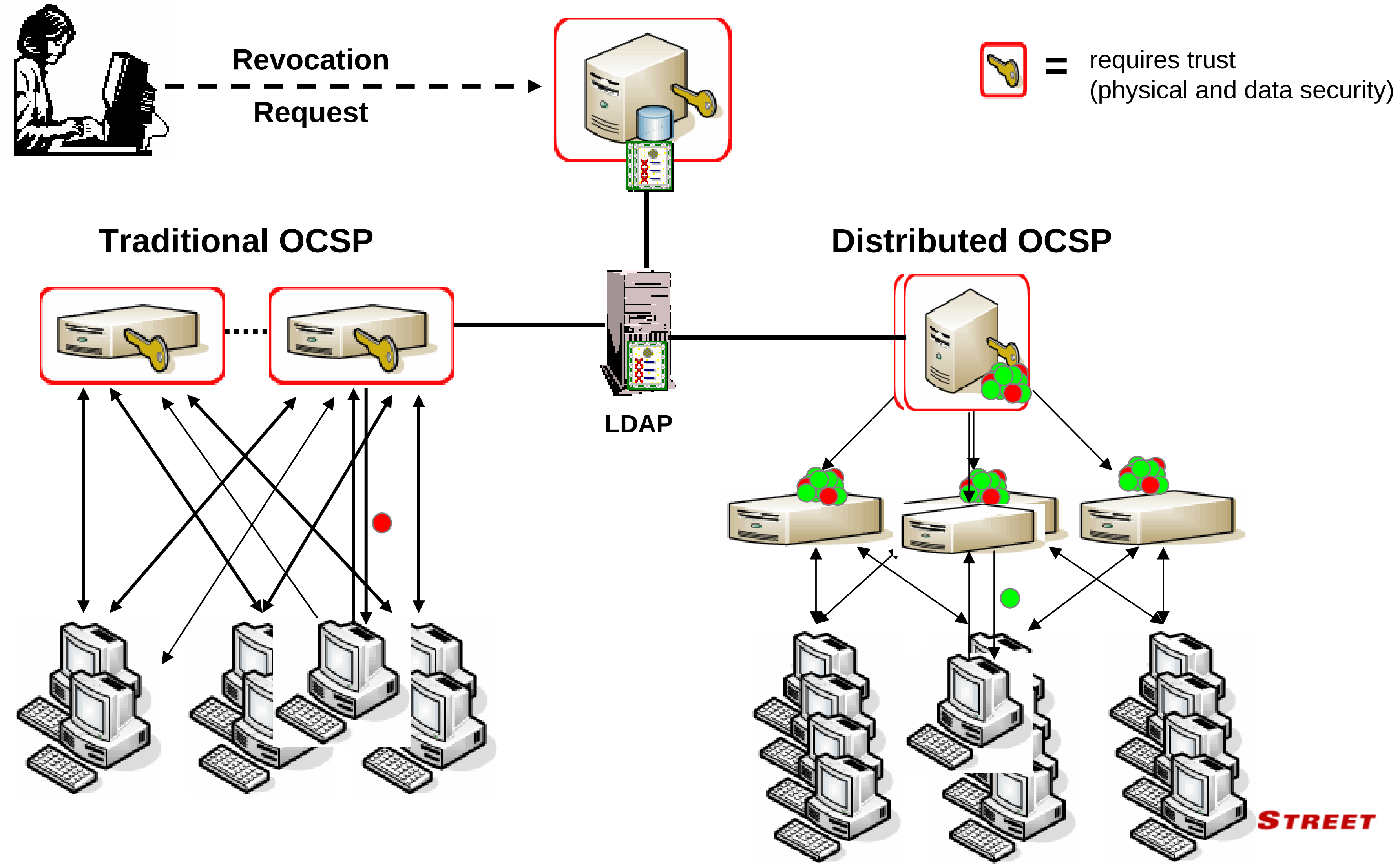
Distributed Validation Architecture

CoreStreet's Unique Design Principle

Design Principle

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

CoreStreet OCSP Validation



Revocation

Request

= requires trust (physical and data security)

Traditional OCSP

Distributed OCSP

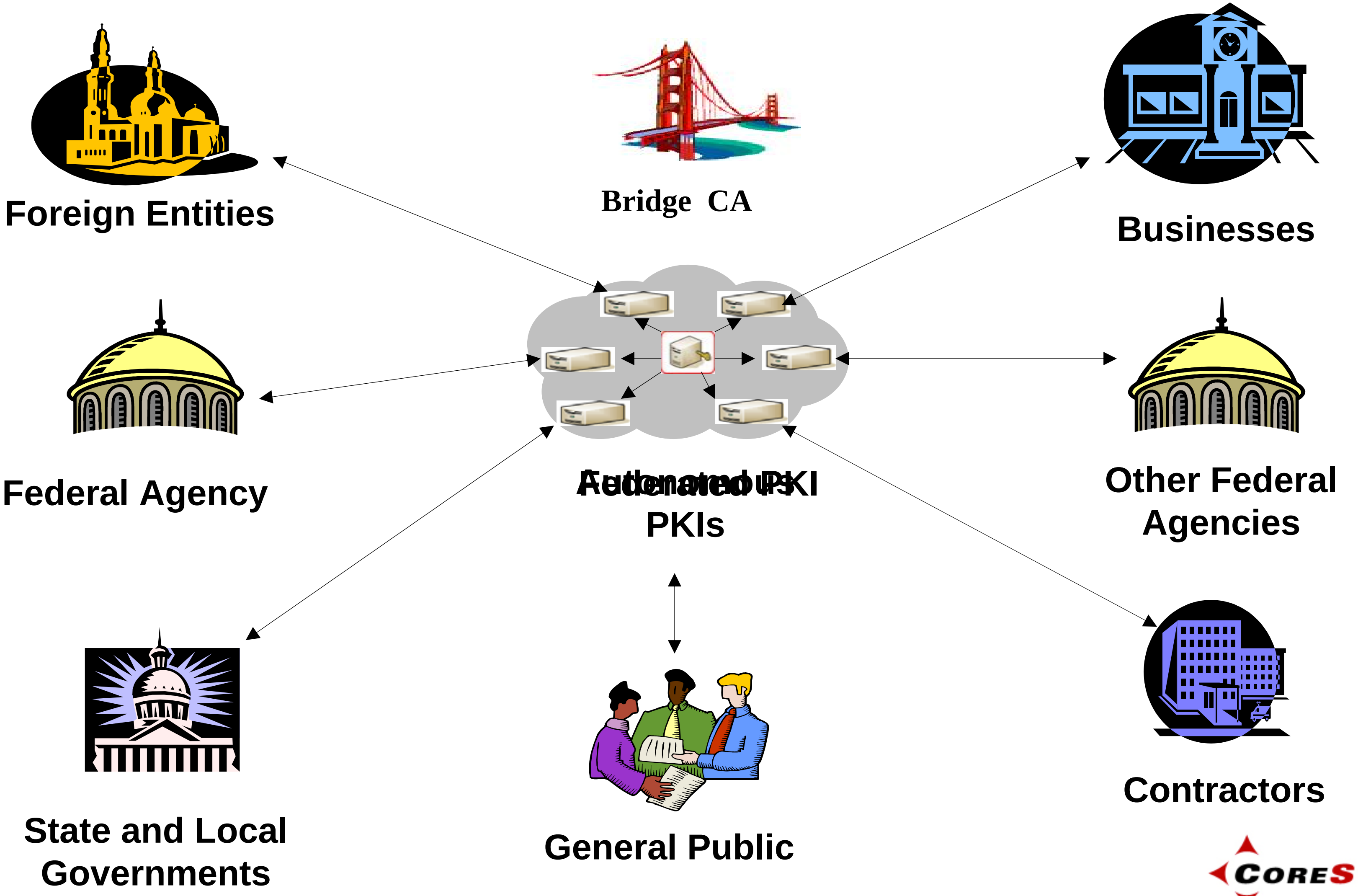
LDAP

Validation Considerations #2

- **Deploy a <u>distributed</u> credential validation service**
  - Required for high performance, availability and scalability
  - More secure approach
  - Less risk - chosen architecture for DoD validation infrastructure
- **Minimize impact on relying party applications**
  - Expensive to install, upgrade or configure desktop
  - Single URL for all validation requests

CoreStreet

Federated Environment = Collection of PKIs



Foreign Entities

Bridge CA

Businesses

Federal Agency

Federated PKI

Autonomous PKIs

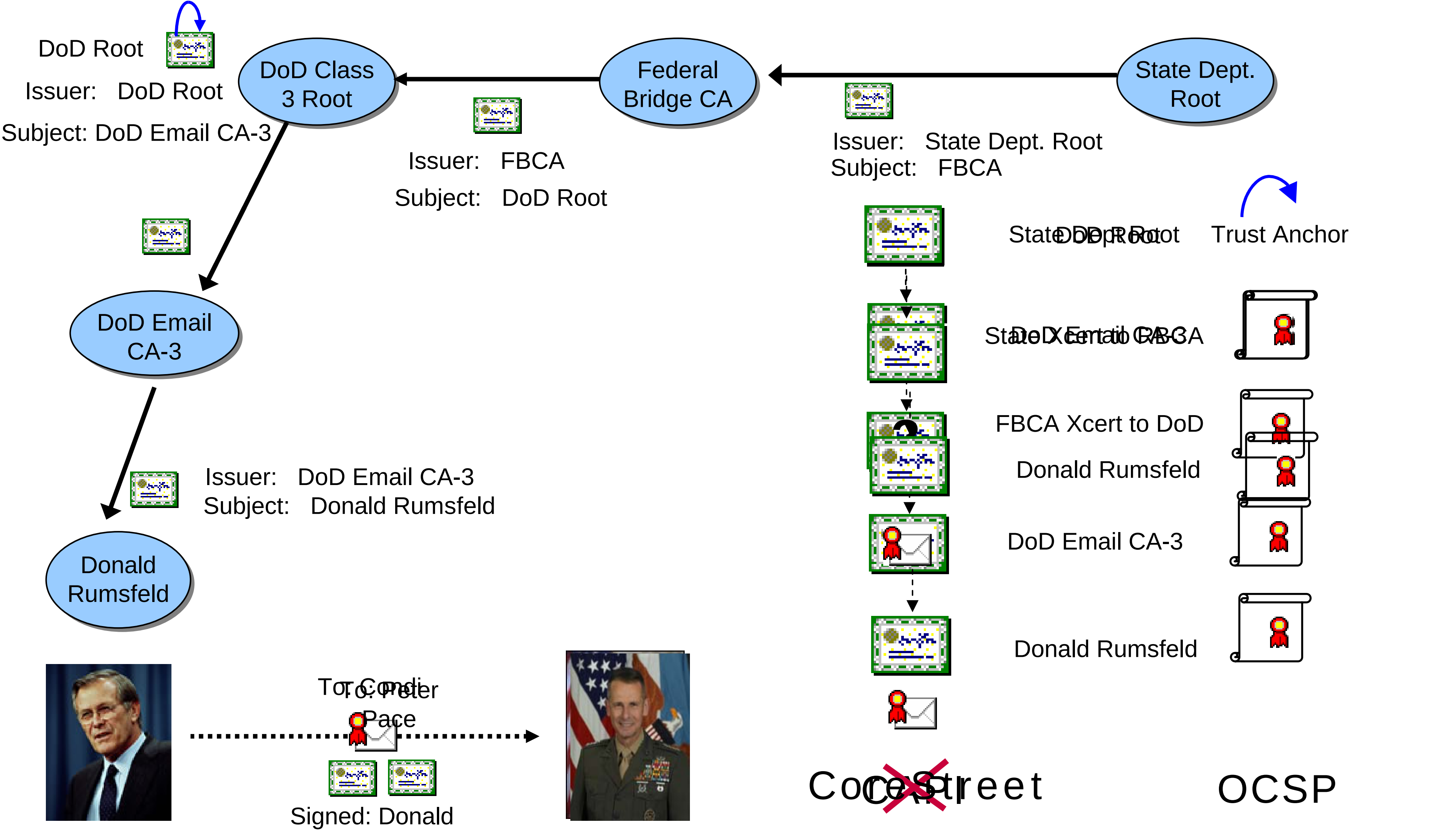
Other Federal Agencies

State and Local Governments

General Public

Contractors

Authentication in Bridge Environment



DoD Root

Issuer: DoD Root

Subject: DoD Email CA-3

Issuer: FBCA

Subject: DoD Root

Issuer: State Dept. Root

Subject: FBCA

Issuer: DoD Email CA-3

Subject: Donald Rumsfeld

To: Condi

To: Peter Pace

Signed: Donald

State Dept. Root

DoD Root

Trust Anchor

State Xcert to FBCA

DoD Email CA-3

FBCA Xcert to DoD

Donald Rumsfeld

DoD Email CA-3

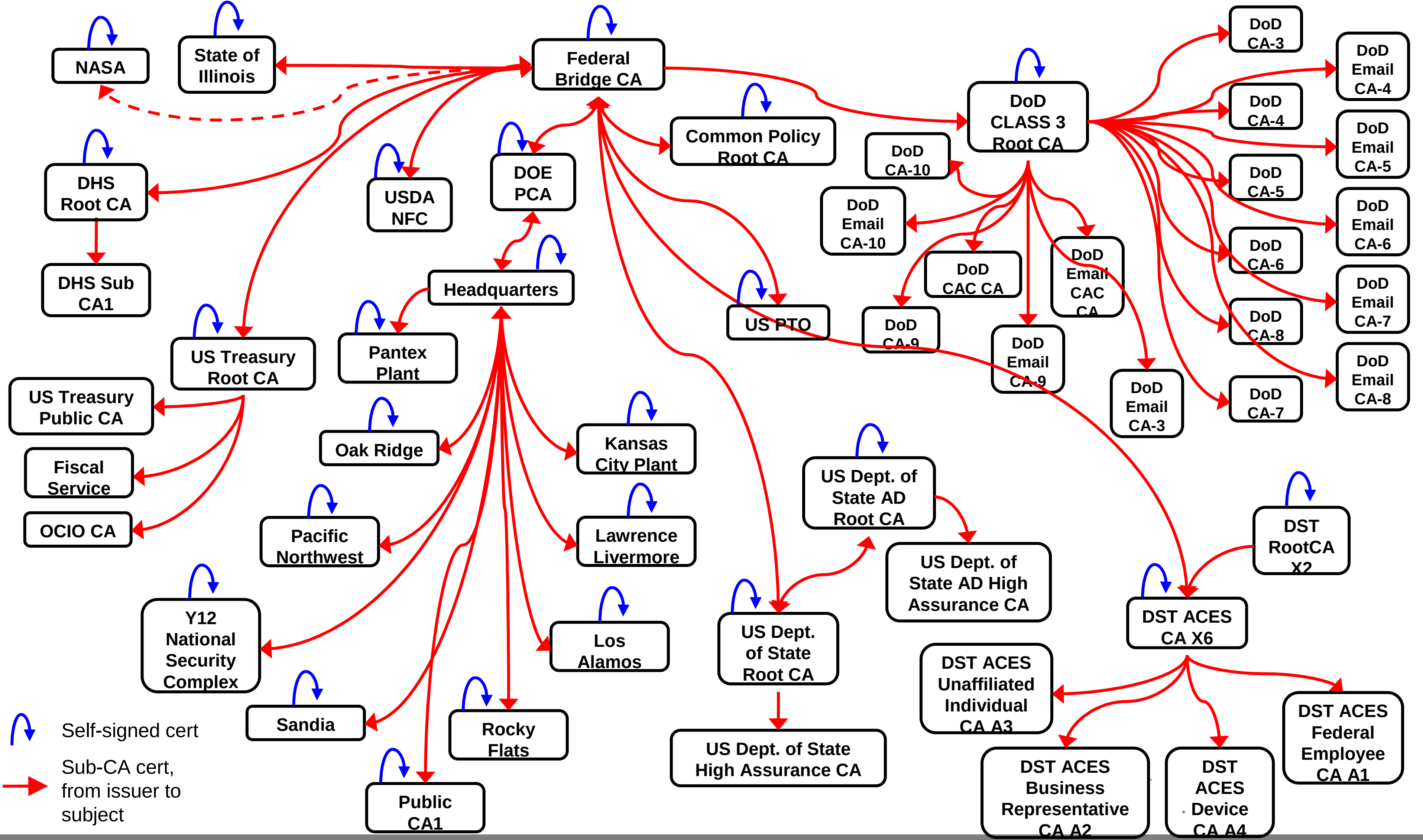
Donald Rumsfeld

CoreStreet

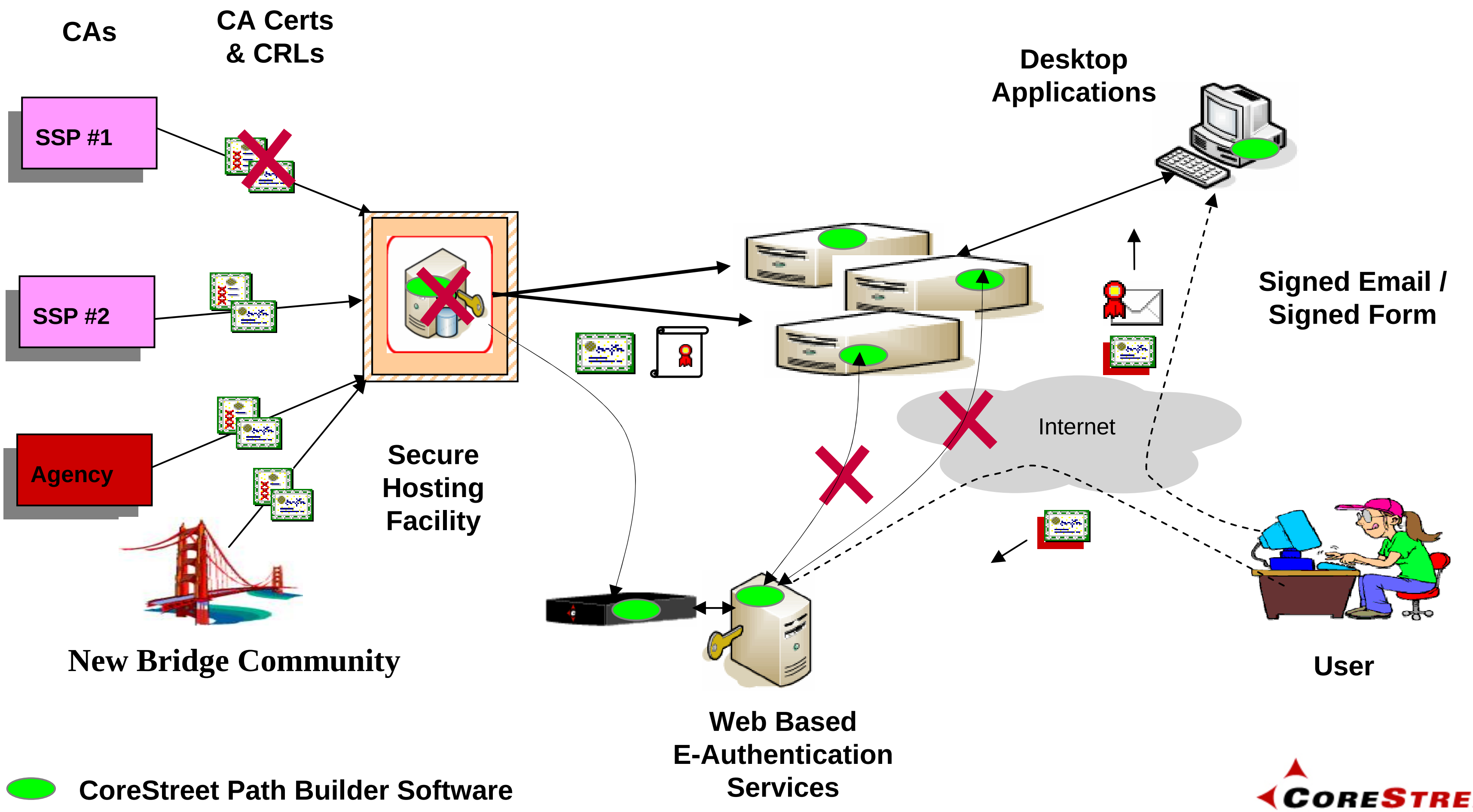
~~CA~~

OCSP

The Federal Bridge Environment



CoreStreet Path Builder System



CORESTREET

Validation Considerations - #3

- **Architecture must support uninterrupted service**
  - Distributed approach is best choice
- **Validation must be available to all relying parties**
  - Analogous to DNS implementation
- **Minimize impact on relying party applications**
  - Minimize number of trust points at the relying party application
- **Additional benefits of federal bridge model**
  - Central control of validation policies and constraints
  - Automated enforcement of path constraints

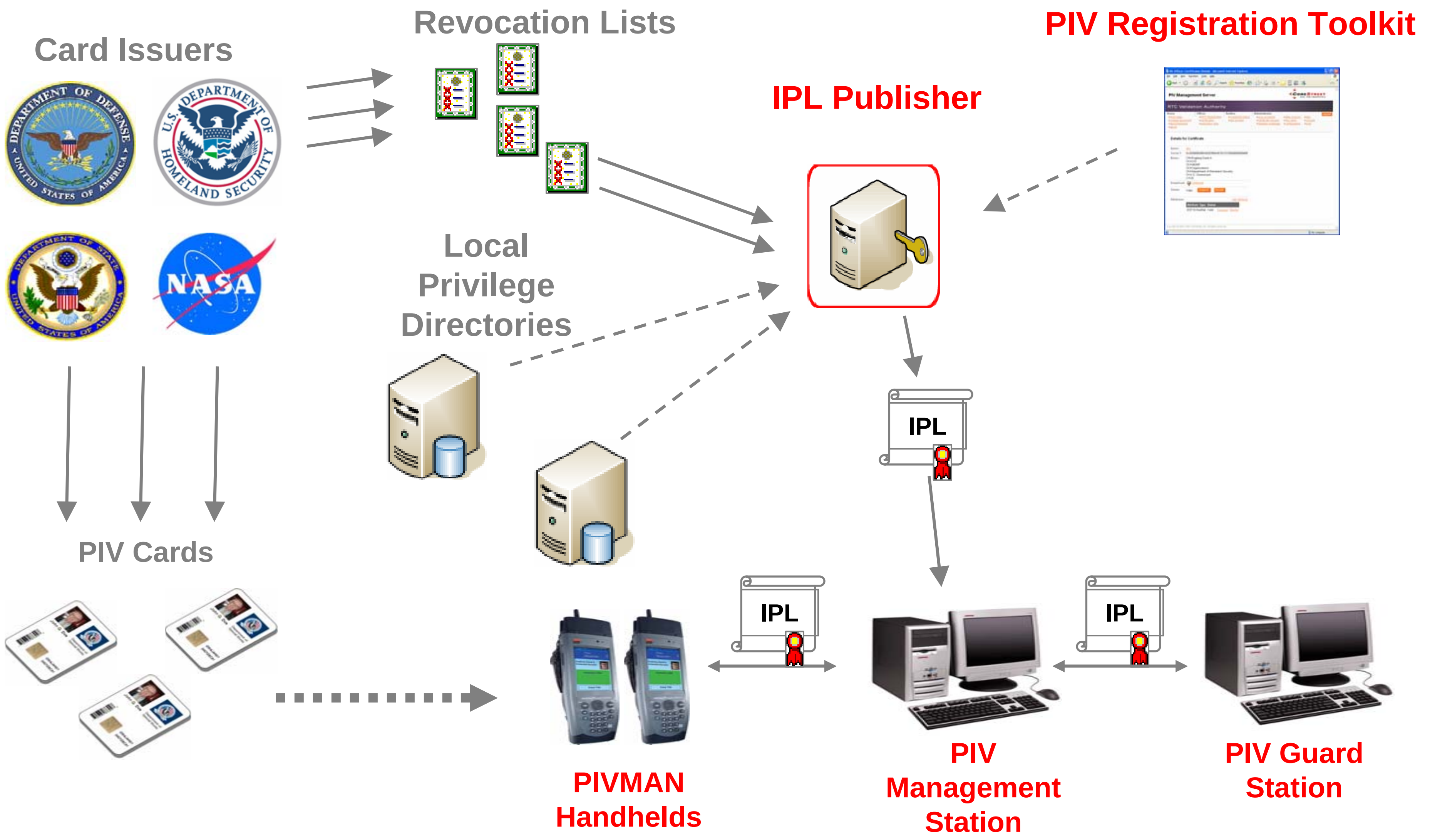
CoreStreet

Privilege Validation – every day & the day

- Are you who you say you are?
- Should you be allowed in (right people at right time)?
- Do you know who entered the area and when?
- Do you know who has left the area and when?

CoreStreet

PIVMAN System



CAC or PIV for ID Checking: Authentication

Step 1: Read certificate

Step 2: Validate certificate

Step 3: Challenge PIN

Step 4: Confirm PIN

Step 5: Challenge Private Key

Step 6: Verify Private Key Operation

Step 7: Read biometric(s)

Step 8: Match biometric(s)

Step 9: Display roles/privileges

CoreStreet

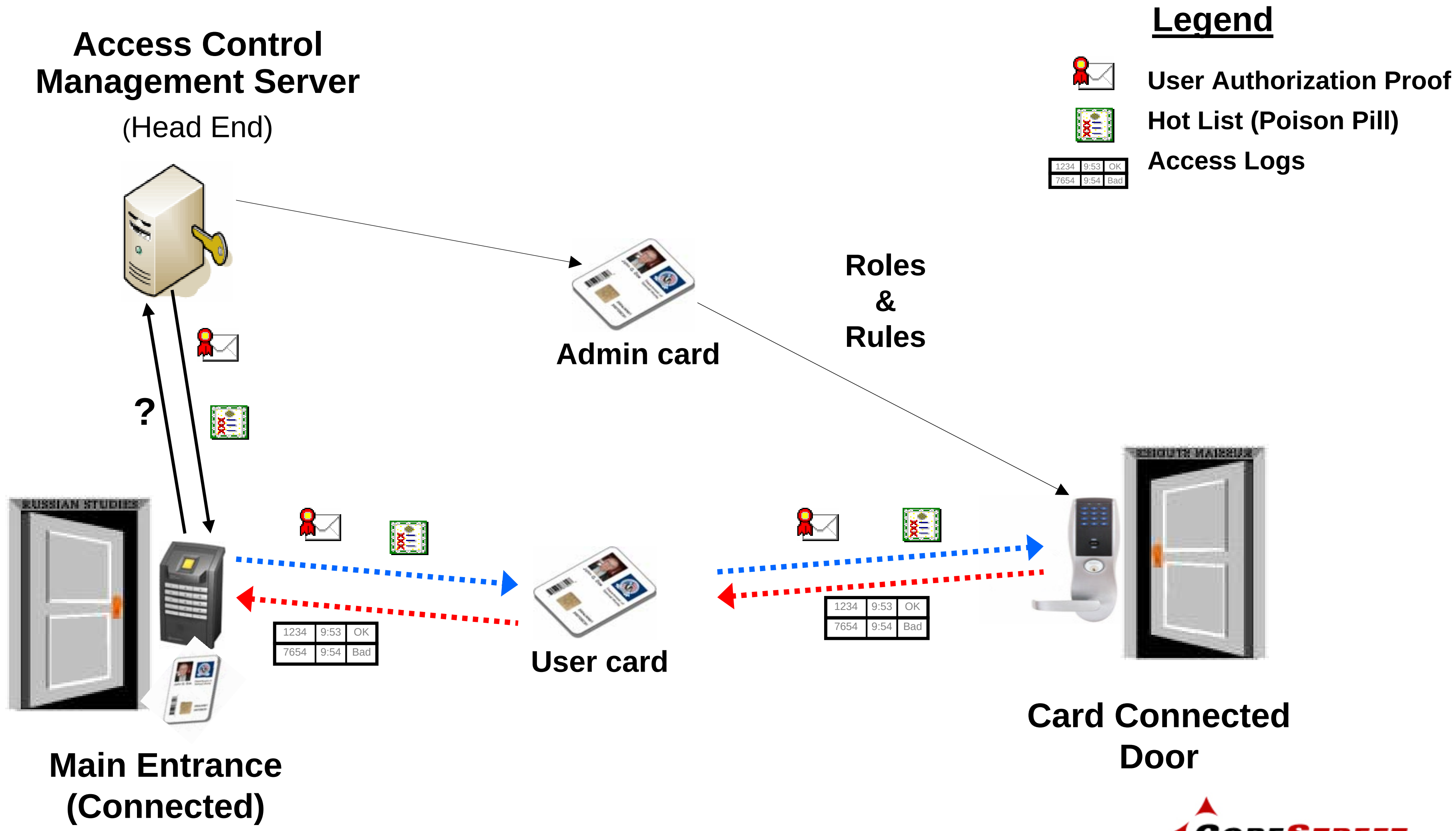
Validation Considerations - #4

Extending your PIV card's operational usability:

- **Include optional facial image**
  - Digitally signed ensures integrity
  - Easy to use to authenticate visually
- **Include contactless Card Authentication Certificate**
  - Reading certificate from contact chip is slow

CoreStreet

Card Connected Physical Access



Access Control Management Server

(Head End)

Admin card

Roles & Rules

?

User card

Main Entrance (Connected)

Card Connected Door

1234	9:53	OK
7654	9:54	Bad

1234	9:53	OK
7654	9:54	Bad

Legend

- User Authorization Proof
- Hot List (Poison Pill)
- Access Logs

1234	9:53	OK
7654	9:54	Bad

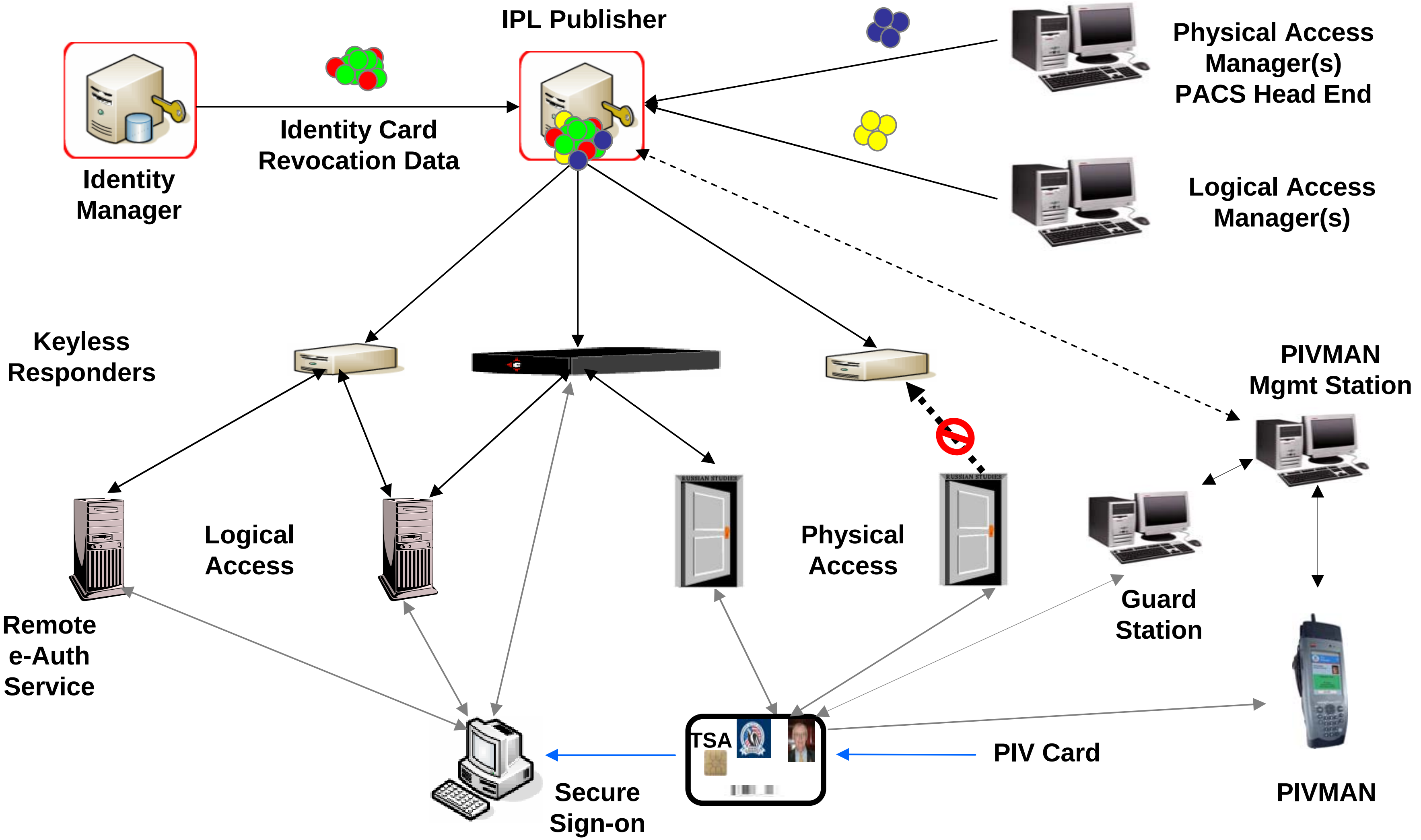
CoreStreet

Validation Considerations - #5

Extending your PIV card’s usability:

- **Include contactless Card Authentication Certificate**
  - Enables future “strong” authentication uses of card
- **Reserve storage container for physical access**
  - 2-3 kB for roles/privileges/attributes/audit logs
- **Recommend NOT tying PACS to your IDMS**
  - Strong authentication can be done with card alone

Summary of Benefits of HSPD-12



CoreStreet Product Summary

- **OCSP Solution**
  - Validation Authority, Desktop & Server Validation Clients, keyless Responder Appliance
  - Only NIAP certified Validation Authority on market today – EAL 3+
- **Path Builder System**
  - Path building and revocation checking for federated PKIs
  - Client side products for enabling applications
- **PIVMAN System**
  - Mobile and guard station privilege checking
- **Physical Access Solution**
  - Merging physical & logical access control with single credential

CoreStreet PKI Toolkit

CoreStreet royalty free SDKs

- PKI Toolkit (“C” and Java)
- Provide low level routines for
  - Sending/receiving OCSP & SCVP requests/responses
  - RFC 3280 path validation
  - Policy & name constraint processing
- Officially certified by GSA’s e-Authentication lab

For additional information:

- Bob Dulude
- Chief Security Officer

- Mobile: (781) 710-0436
- Office: (617) 661-3554 x202
- Email: bob@corestreet.com

- Website
- www.corestreet.com
- Corporate Headquarters

One Alewife Center
Suite 200
Cambridge, MA 02140

CoreStreet