Cybertrust SSP Implementations Lessons Learned NIST PKI Workshop

April 11, 2006

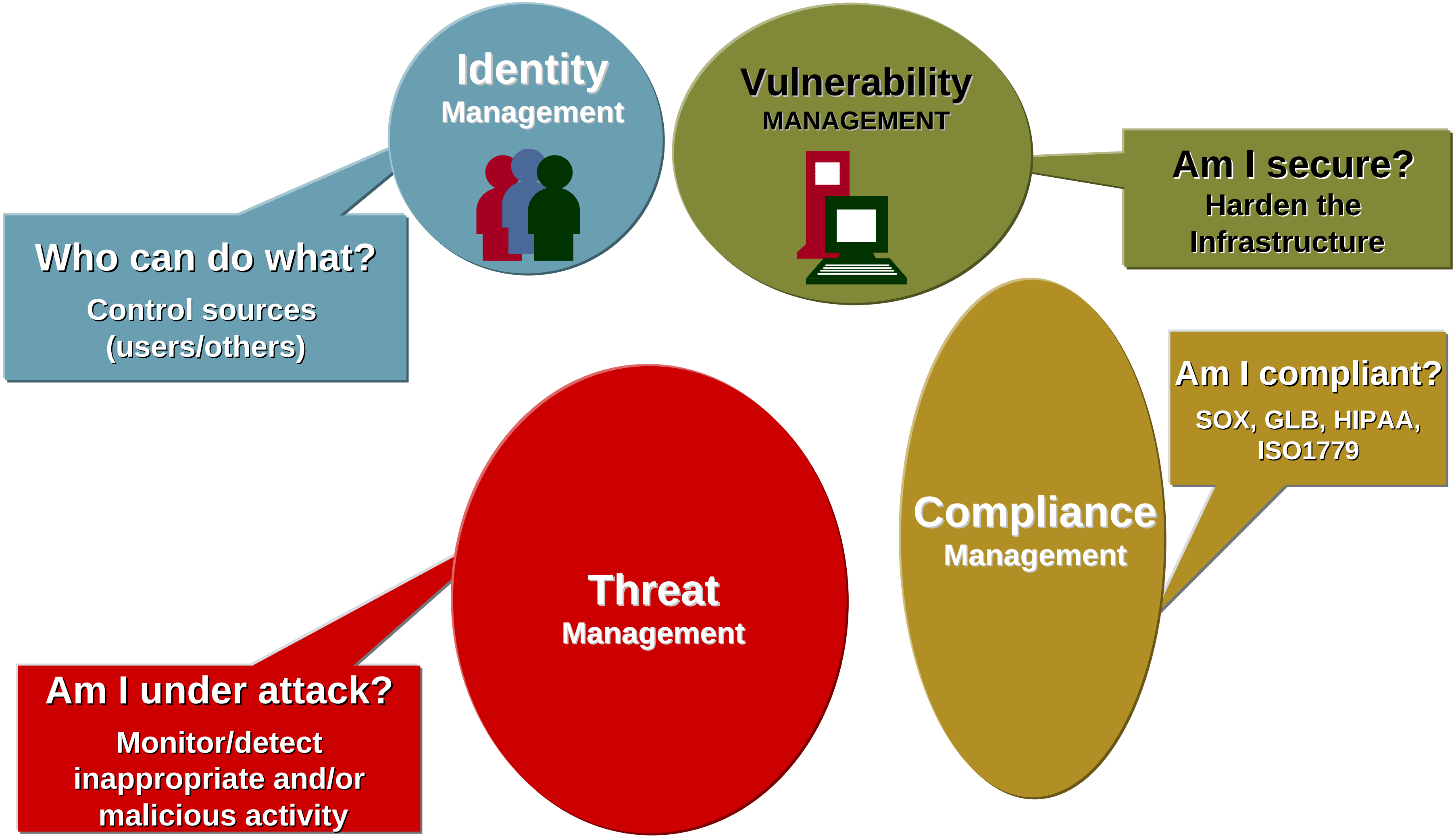
Agenda

Who is Cybertrust?

Meeting the Requirements of FIPS-201

SSP Implementation Options

Current IT Security Challenges



Identity Management

Who can do what?

Control sources (users/others)

Vulnerability MANAGEMENT

Am I secure?

Harden the Infrastructure

Compliance Management

Am I compliant?

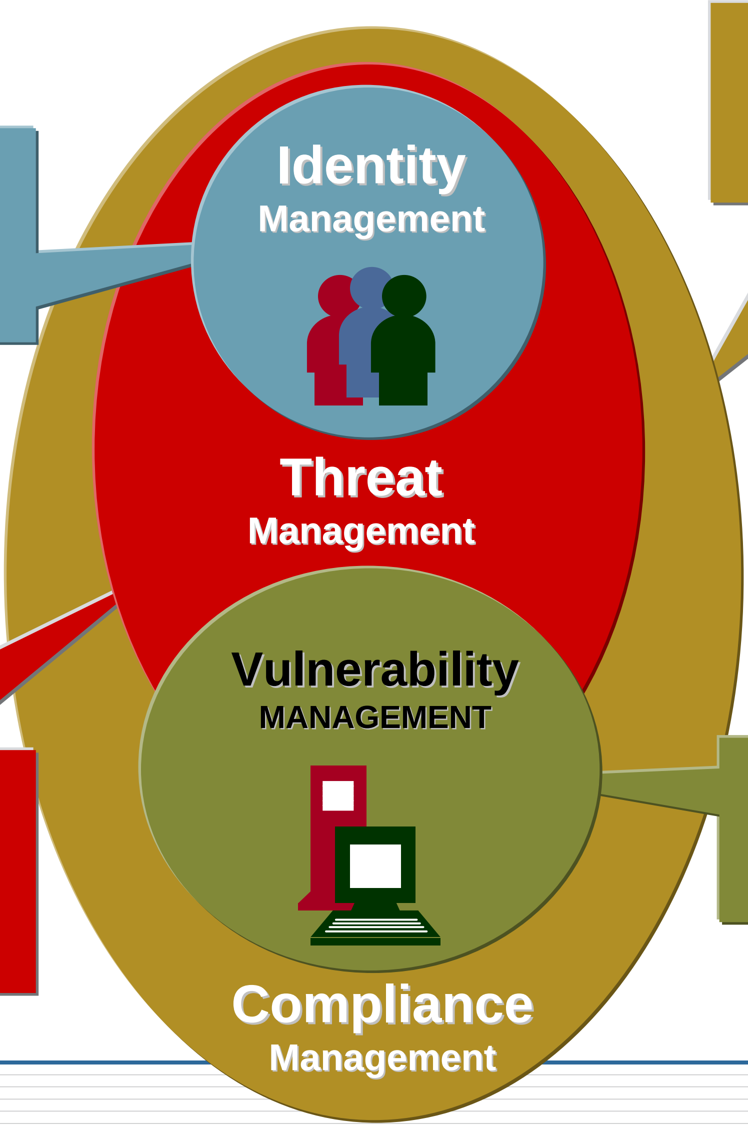
SOX, GLB, HIPAA, ISO1779

Threat Management

Am I under attack?

Monitor/detect inappropriate and/or malicious activity

Integrated Risk Management



Who can do what?

Control sources (users/others)

Am I compliant?

SOX, GLB, HIPAA, ISO1779

Identity Management

Threat Management

Vulnerability MANAGEMENT

Compliance Management

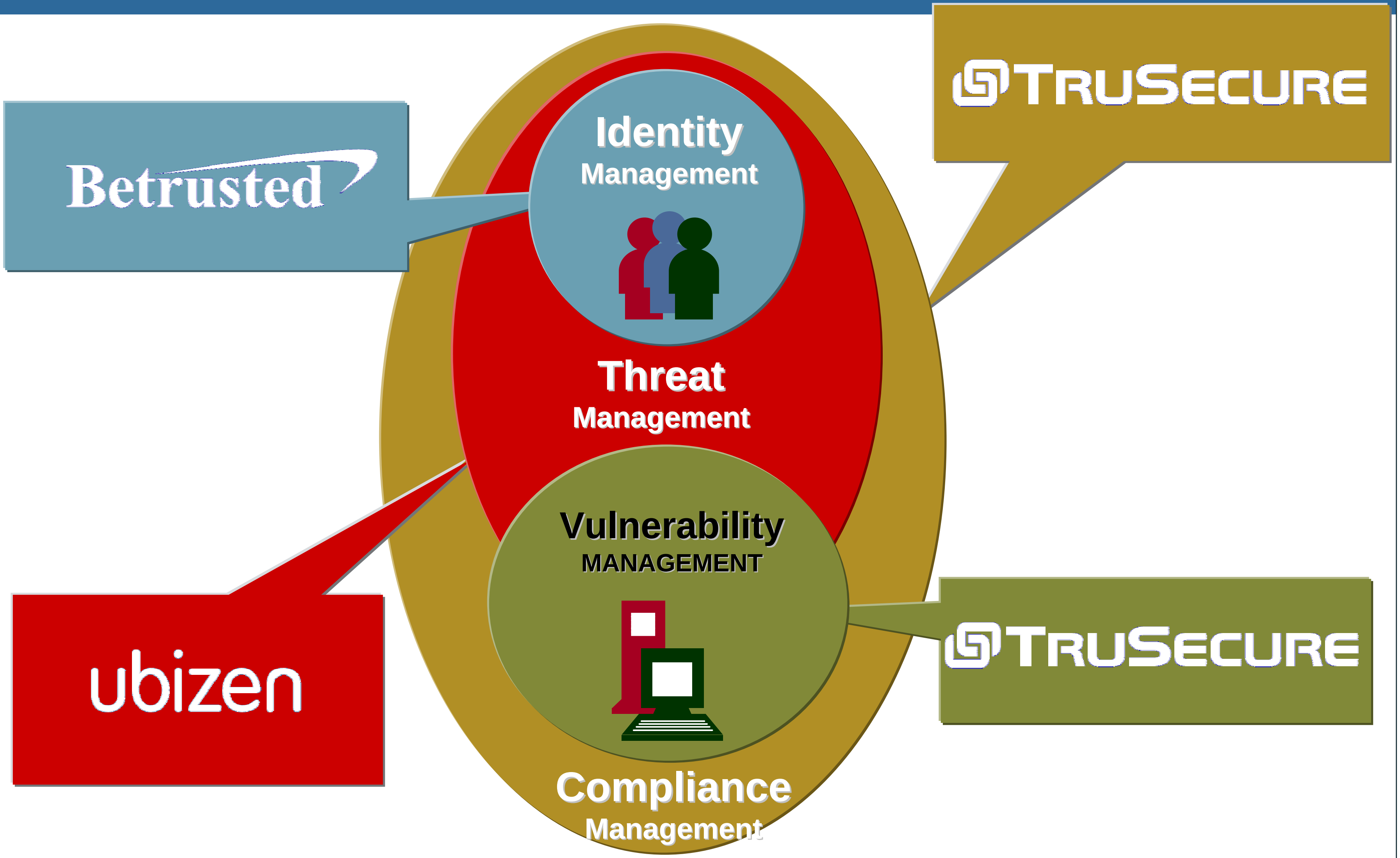
Am I under attack?

Monitor/detect inappropriate and/or malicious activity

Am I secure?

Harden the Infrastructure

Integrated Risk Management



Who is Cybertrust?

Created Through Merger of Three Industry Leaders

Betrusted Ubizen Trusecure

Establishes the first global security company that can provide:

- Consistent, multi-disciplined security strategy
- Global presence, local service
- Lifecycle security and compliance solutions
- Deep security expertise and real-time global intelligence

Who is Cybertrust?

We are 100% focused on security and can work with any security products or vendors.

We have predicted – and warned our customers of – every major security event in the last seven years.

We scan more than six million internal and external IP addresses and devices quarterly

We monitor more than 11,000 hackers daily

Our capabilities and solutions can be delivered through:

- Professional services
- Managed services (utilizing an enterprise software platform at a customer's site or through multiple, accredited "Trustcenters" located throughout the world)
- Products/technology

Who is Cybertrust?

Our independent intelligence division, ICSA Labs®, has tested, certified, and strengthened over 95% of the installed security products on the market today.

Our global presence ensures consistent worldwide coverage and measurement.

We have a world-class consulting team which includes many of the visionaries who shaped the information security industry.

We partner with thousands of customers worldwide, including more than half of the Fortune 50 companies.

Who is Cybertrust?

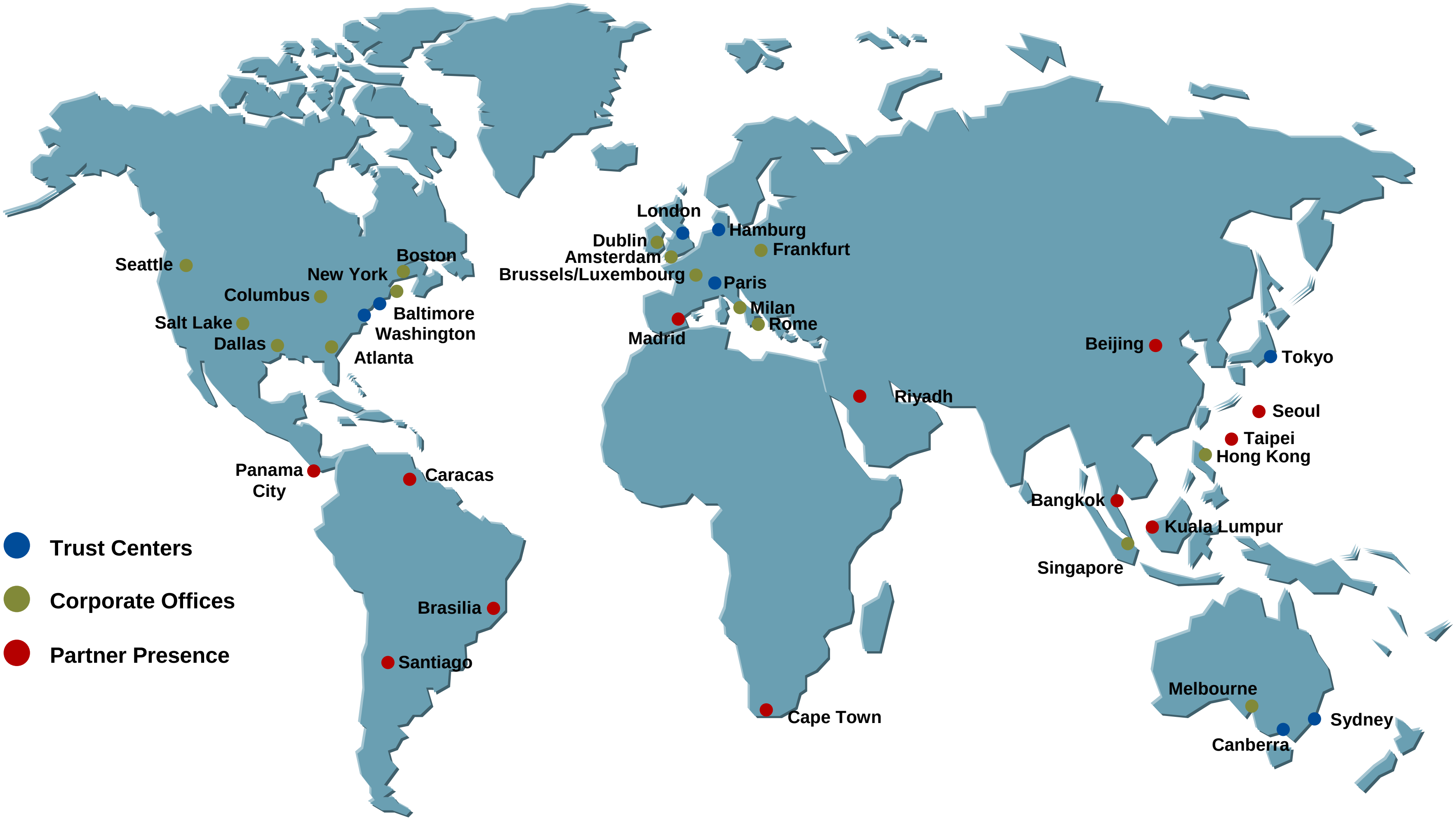
Provide identity management and hosted services to Belgium for National ID card to 8 million residents

- 3 million ID cards issued to date with a 5 year lifetime

E-Passport Australia

Host NATO CA in our Trust Center in Leuven, Belgium

Global Presence - *Local Service*



● Trust Centers

● Corporate Offices

● Partner Presence

Cybertrust SSP

Policies Driving Need for Higher Levels of Security and Improved Credentials

- Presidential Directive HSPD-12 and FIPS 201
- GSA Creation of Federal SSP Program
- Office of Management and Budget (OMB) Compliance mandates for security
- Government Paperwork Elimination Act (GPEA)
- FISMA and resulting NIST standards
- E-Authentication, PKI bridge initiatives and the goal of interoperability with Commercial entities and efforts, e,g., SAFE, Certipath, and Higher Education efforts e.g., HEBCA, Shibboleth

Cybertrust and Federal Government Initiatives

Core competencies such as Managed PKI, Identity Management, and Certification and Accreditation (C&A) align with important initiatives within the current Federal environment

Thought leadership within key groups including:

- PKI Technical Working Group
- Electronic Authentication Partnership (EAP)
- IETF
- Path Validation Working Group
- Internet 2

Cybertrust personnel are well positioned within influential communities forwarding and implementing initiatives at the program and agency level

UniCert Certified as interoperable with the Federal Bridge Certification Authority (FBCA)

Current Data Center in Columbia, MD meets or exceeds standards desirable for outsourcing of agency IT functions to secured facilities

Federal Shared Service Providers (SSP) Program

General Services Administration (GSA) Launches Program in March 2004

Cybertrust Certified as a SSP in August 2004

Program Enables Federal Agencies to Leverage Outsourced PKI Services

Facilitates Issuance of Credentials to Agency Employees and Contractors

Supports Objectives of Presidential Directive HSPD-12

Federal Agencies' Use of SSPs mandated by OMB memo M-05-05

Cybertrust Platform Evolution Designed to Meet Market Needs

- Support for Multiple CA Products
- Support for Multiple Card Management Systems
- Hosted Validation Services

Keys to Interoperability

Policy + Technical = Interoperability

Policy → Level of Assurance (LOA):

Certification Policy (CP)

Identity Proofing Requirements

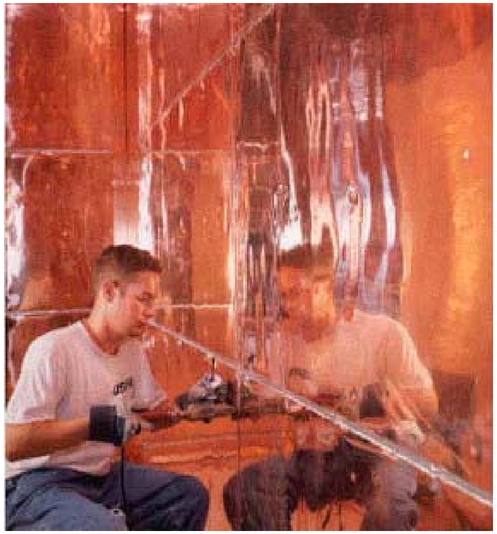
Technical:

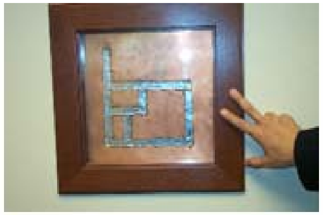
Operations

Storage and/or creation of user keys

CA root keys in Browser

Elements of the Cybertrust SSP Offering





Betrusted Data Center construction, using copper-lined walls with soldered edges to reduce RF Emissions

Access only for cleared personnel, via biometric (hand geometry) and proximity card

Man Traps secure entrances into sensitive Data Center areas

- Hosted in Highly Secure Data Center
- System Monitored on a 24x7x365 basis
- Standard Service Level at 99.5%
- Full Certificate Life-cycle management
- SSP Operations Run Per Approved Certification Practice Statement
- Annual Compliance Audit of System Conducted by certified Third Party Auditor
- System Certification and Accreditation also Performed
- Business Continuity/Disaster Recovery
- System Audit Logging and Off-site Data Archiving
- Help Desk Services

Elements of the Cybertrust SSP Offering

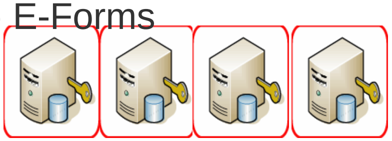
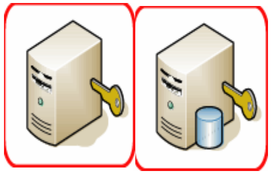
OCSP Support

- Cybertrust can manage the OCSP Responder for Agency Implementations
- Cybertrust is in the process of becoming an approved validation service provider per the E-Authentication Initiative
- Cybertrust would use the Corestreet validation product
  - Used by DOD for OCSP validation
  - In the process of becoming an approved validation product per the E-Authentication Initiative

Directories Supported

- LDAP
- X.500
- Sun1

System Elements

FIPS 201 Cards	Infrastructure Services (SSP)	Integration Services	ID vetting/ Registration	Devices / Systems/Applications
 	(1) Card Management System (CMS) (2) Certificate Authority (CA) (3) Validation Authority (VA) and Privilege Management (4) E-Forms 	(1) Integrate user community HR database (2) Integrate NIMS 	(1) Enrollment/ Issuance stations (2) Identity proofing 	

↑ FIPS 201

↑ FIPS 201
E-Authentication

↑ FIPS 201
(PIV-I)

Agency Experience So Far

Large Agency

- Pre FIPS-201 100,000 + Users Expected to scale to 400,000 when fully deployed
- UniCERT CA on Dedicated Hardware, Hosting CMS, Replicated Authoritative Directory

Medium Agency

- Post FIPS-201 30,000 to 120,000 Users
- UniCERT CA on Shared Hardware, Hosting CMS, Hosting Issuance Directory, Agency Running Authoritative Directory

Small Agency

- Post FIPS-201 3,000 Users
- Hosting Microsoft CA, Selective Push of Identity Information to Shadow Domain Hosted at Cybertrust, CMS Hosted at Cybertrust

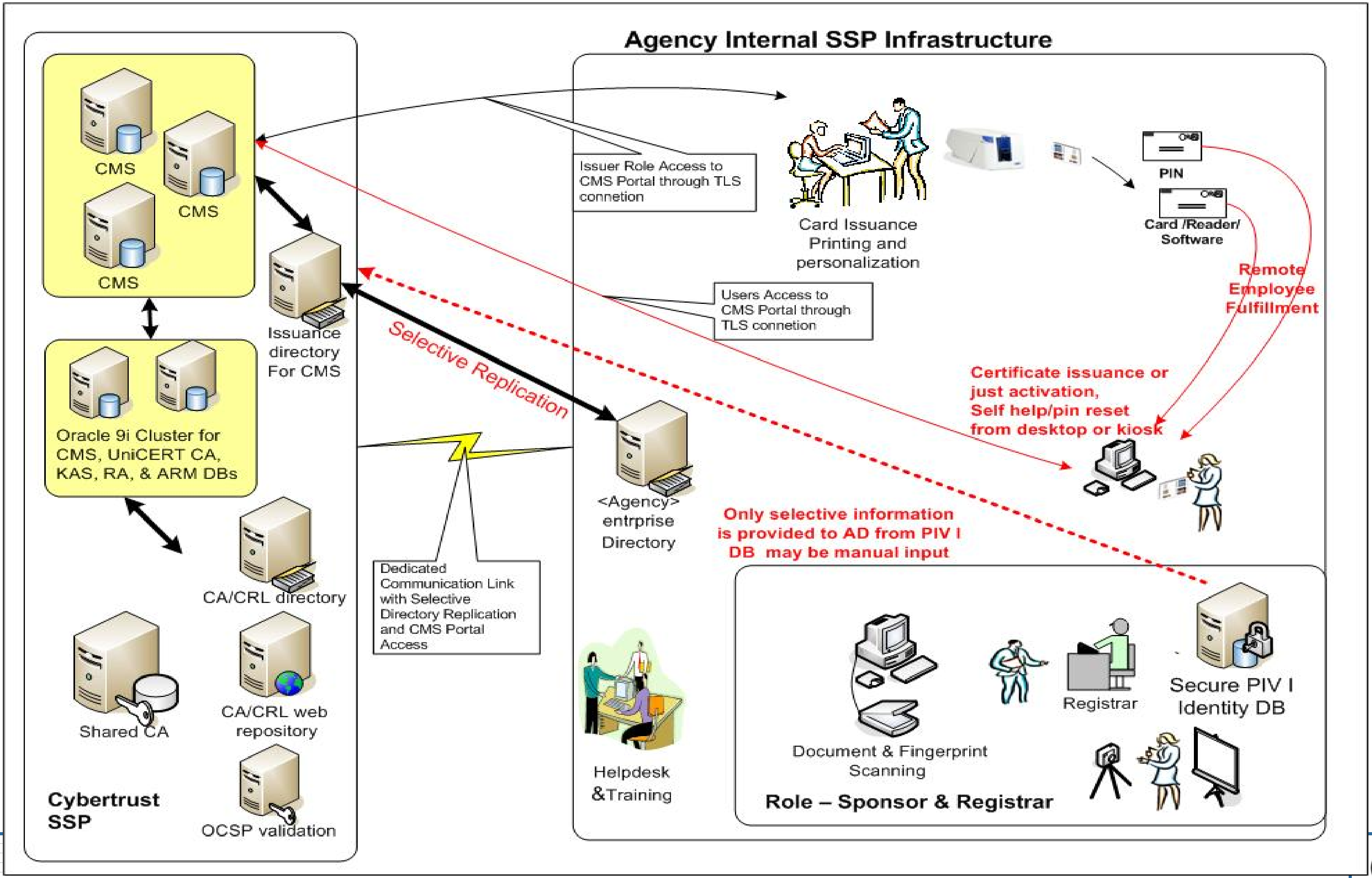
Cybertrust Deployments and Partners

Integrators	Identity Management System (IDMS)	Card Management System (CMS)	Validation	Card Printing System	Government Agency/ Commercial Customer
Anteon	Probaris	ActivIdentity	Corestreet	Oberthur	Medium Size Agency
Anteon	Infomosaic	ActivIdentity	Corestreet	Oberthur	MDOT for WinterFox and First Responders
Authsec	TBD	ActivIdentity	Corestreet	Gemplus	Large Government Agency
Microsoft	IdNexus	Alacris	Microsoft	Gemplus	Small Government Agency

Other Partners:
Systems Research Applications, Inc (SRA) [Integrator]
Actcom [Integrator]
Lockheed Martin [Integrator]
Others being added!

- Intercede [CMS]
- Tumbleweed [Validation]
- Infomosaic, Corestreet [toolkit]

Outsourced PKI - Cybertrust Hosting Agency Equipment (Example)



Agency Internal SSP Infrastructure

CMS

CMS

CMS

Issuance directory For CMS

Oracle 9i Cluster for CMS, UniCERT CA, KAS, RA, & ARM DBs

CA/CRL directory

Shared CA

CA/CRL web repository

OCSP validation

Cybertrust SSP

Issuer Role Access to CMS Portal through TLS connetion

Card Issuance Printing and personalization

PIN

Card /Reader/ Software

Remote Employee Fulfillment

Users Access to CMS Portal through TLS connetion

Selective Replication

Certificate issuance or just activation, Self help/pin reset from desktop or kiosk

<Agency> entrprise Directory

Only selective information is provided to AD from PIV I DB may be manual input

Dedicated Communication Link with Selective Directory Replication and CMS Portal Access

Helpdesk &Training

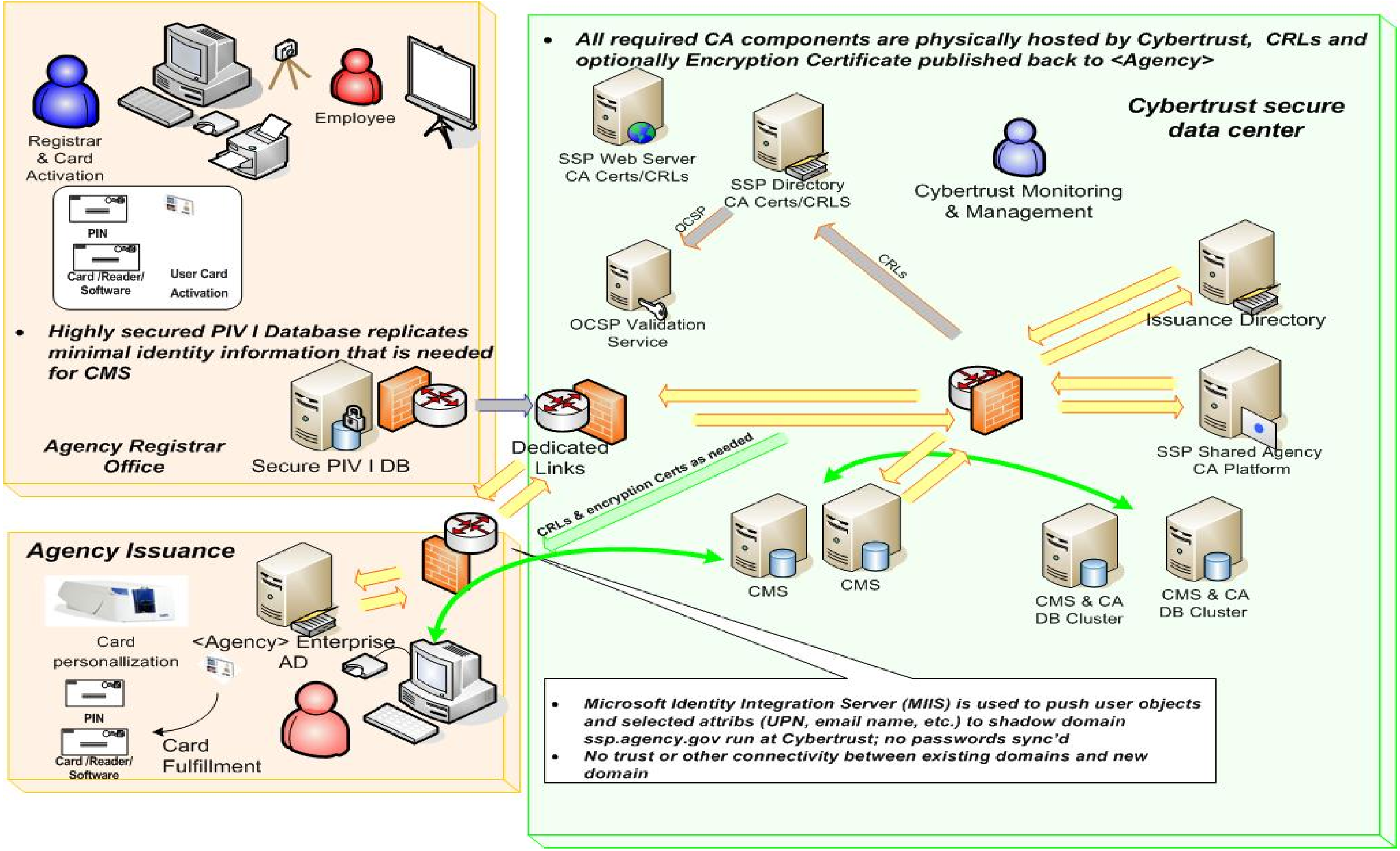
Registrar

Secure PIV I Identity DB

Document & Fingerprint Scanning

Role – Sponsor & Registrar

Outsourced PKI – Example Cybertrust Hosting Agency Equipment (Data Flow)



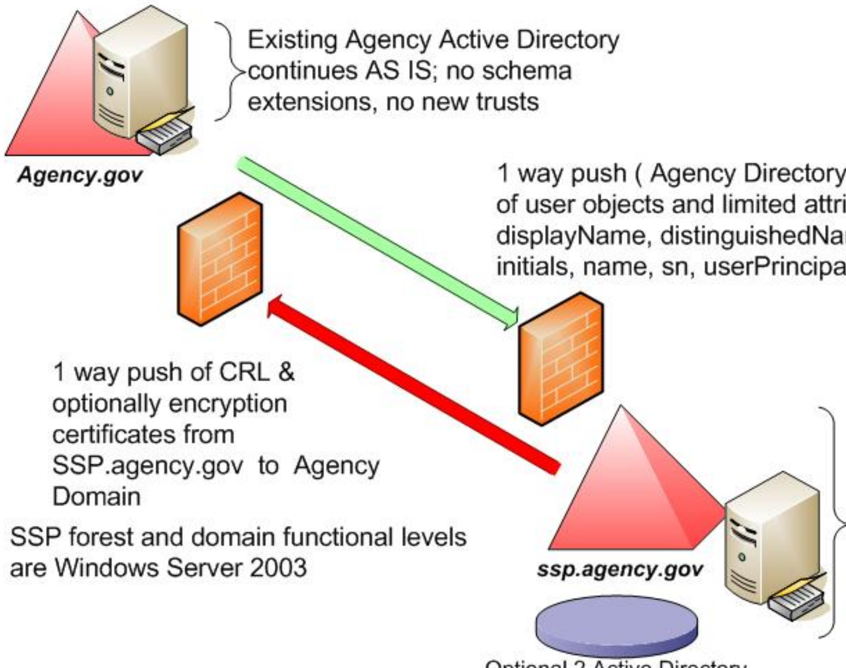
- *All required CA components are physically hosted by Cybertrust, CRLs and optionally Encryption Certificate published back to <Agency>*

- *Highly secured PIV I Database replicates minimal identity information that is needed for CMS*

- *Microsoft Identity Integration Server (MIIS) is used to push user objects and selected attribs (UPN, email name, etc.) to shadow domain ssp.agency.gov run at Cybertrust; no passwords sync'd*
- *No trust or other connectivity between existing domains and new domain*

Example of Authoritative Directory Model

Directory Infrastructure for Agency and Related Agency for SSP Support



Existing Agency Active Directory continues AS IS; no schema extensions, no new trusts

1 way push (Agency Directory to <Agency> SSP) of user objects and limited attribute set: (cn, displayName, distinguishedName, givenName, initials, name, sn, userPrincipalName etc.)

1 way push of CRL & optionally encryption certificates from SSP.agency.gov to Agency Domain

SSP forest and domain functional levels are Windows Server 2003

New forest created at Cybertrust SSP that shadows agencies production forest; contains only those objects and attributes required to create certificates

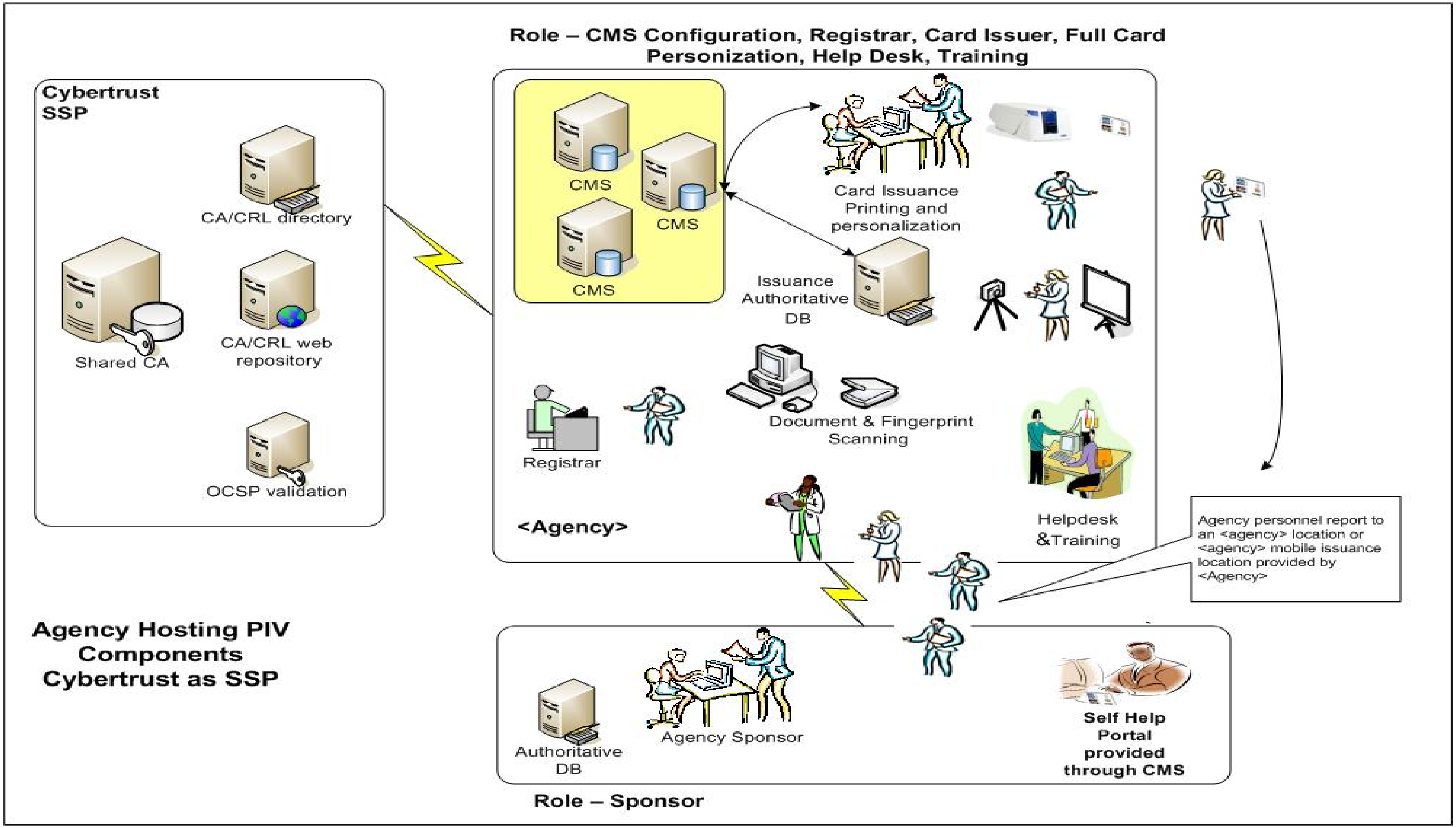
Optional 2 Domain Controllers for the SSP Agency domain; DCs

Optional 2 Active Directory site for redundancy

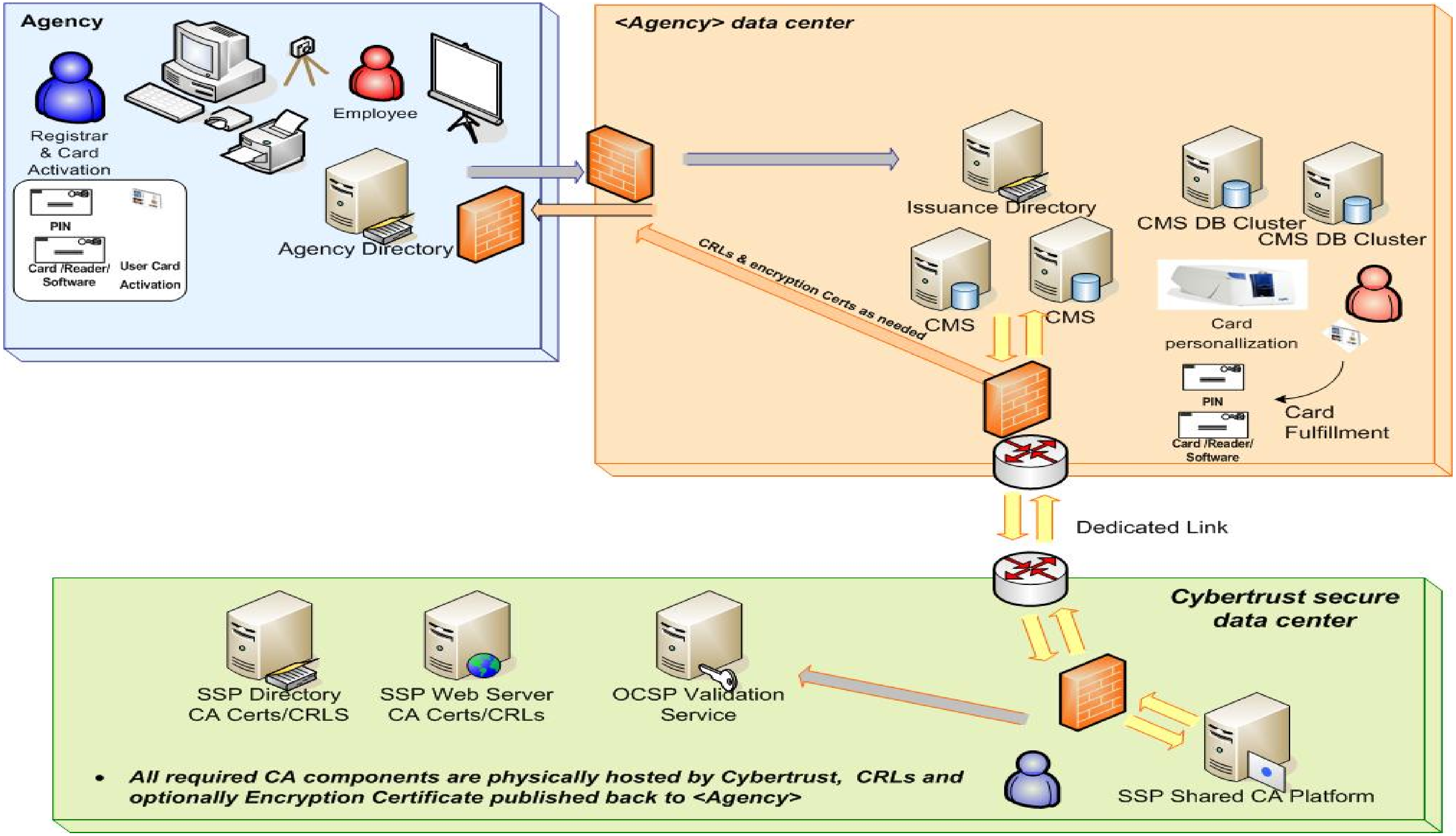
- ***Microsoft Identity Integration Server (MIIS) is used to push user objects and selected attribs (UPN, email name) to domain run at <Agency>; no passwords sync'd***
- ***Current Agency Active Directory exists 'as is' for non AD environments (MIIS) will need to be licensed to support the push from other directory manufacturers***
- ***No trust or other connectivity between existing domains and new domain***

All Agency SSP forest domain controllers run Windows Server 2003 Enterprise Edition with Service Pack 1

Outsourced PKI with Agency Hosted CMS (Example)


Role – CMS Configuration, Registrar, Card Issuer, Full Card Personization, Help Desk, Training
Cybertrust SSP
CA/CRL directory
Shared CA
CA/CRL web repository
OCSP validation
CMS
CMS
CMS
Card Issuance Printing and personalization
Issuance Authoritative DB
Registrar
Document & Fingerprint Scanning
Helpdesk &Training
<Agency>
Agency personnel report to an <agency> location or <agency> mobile issuance location provided by <Agency>
Agency Hosting PIV Components Cybertrust as SSP
Authoritative DB
Agency Sponsor
Self Help Portal provided through CMS
Role – Sponsor

Outsourced PKI with Agency Hosted CMS (Data Flow)



- *All required CA components are physically hosted by Cybertrust, CRLs and optionally Encryption Certificate published back to <Agency>*

Lessons Learned– Issues to Keep in Mind

Pilot vs. Preproduction environment. (Cost, Planning, Time to Deployment Issues)

Proper Organization Composition, Delegation and Cooperation of the Agency HSPD 12 team is strongly recommended to speed decisions

A Technical and Policy evangelist within the agency is useful to educate the internal teams (HR, Security and IT)

Develop your RPS and KRPS *with* the SSP due to the Policy implications with the SSP

Use an Identity Management System (E.g. Sun, CA, IBM) to feed the Card Management System's Issuance Directory

Standardizing the Issuance Directory schema across the Department and its agencies will reduce vendor integration costs.

Minimize card layouts and differences of the print layout to streamline the rollout (Card Printing Is NOT Trivial)

Operate the CMS at the SSP to minimize CMS to CA communications issues and to improve Operational Management

Consider including the Signing and Key Management certificates in addition to the PIV Authentication Certificate

Distributed printing versus centralized printing

Be Sure to Address Business Continuity– Both Disaster Recovery and Vendor Stability

Bottom Line

Setup, configuration and operational testing takes time due to the CA and CMS and Smart card security requirements

Conclusion

“Rome wasn’t built in a day …..

And neither is a FIPS 201 compliant PKI.”

Anonymous

“A good plan executed today is better than a perfect plan executed tomorrow”

George Patton

For More Information

Cybertrust Federal Services Team

Thomas J. Greco
VP Enabling Infrastructures
Tom.greco@cybertrust.com
443-367-7052

Deborah “Debb” Blanchard
Senior Program Manager
Deborah.Blanchard@cybertrust.com
443-367-7011

Russel Weiser
Senior Security Architect
Russ.Weiser@cybertrust.com
801-631-1685