PIV Card based Identity Assurance in Sun Ray & IDM Environment

Ramesh Nagappan
Sun Microsystems
ramesh.nagappan@sun.com

PIV Credentials – What is in your PIV card ?

FIPS-201 Mandatory and Optional On-Card Credentials

Mandatory Credentials

- PIN (Personal Identification Number)
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Two biometric fingerprints (CBEFF)

Optional Credentials

- An asymmetric key pair and corresponding certificate for digital signatures
- An asymmetric key pair and corresponding certificate for key management
- Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Symmetric key(s) associated with the card management system

Source: GSA USAccess

Sun Rays In a PIV Environment

Security

Manageability

Reliability

Mobility

Value

Sun Ray supports the use of PIV Cards

Rationale

PIV card based Identity Assurance in Sun Ray Environment

- Mobility with Security
  - In accordance with HSPD-12/FIPS-201 Logical access control requirements.
  - Use PIV card credentials for Desktop authentication and single sign-on (SSO) of IT systems and applications.
  - PIV card based Hot-desking and secure LAN/WAN access
- PIV credentials based Multi-factor authentication as equivalent to face-to-face verification of a person.
  - Combining Smart card based PIN and PKI Certificates for authentication against FBCA or Agency's PKI authority.
  - Combining Match-to- PIV card Biometric authentication with traditional authentication schemes such as username/passwords.
  - Stronger authentication using random challenges with biometric fingerprints.
- Mission-critical availability with high degree of Identity assurance.

PIV based Logical Access Control

Sun OpenSSO
Web SSO/Federation

PIV Credentials based Logical Access Control

Sun Ray Technology

Sun Technologies for PIV

Integration with PIV Smart card / Biometric authentication middleware

- Sun Ray Desktops
  - Verified integration with PIV Smartcard based PKI/Biometric authentication providers.
  - Verified integration with USB based Biometric scanners
  - Desktop authentication for Solaris/Solaris Trusted Extensions and Linux (using PAM) and Microsoft environment (using GINA).
  - Multi-factor authentication support combining Biometrics with Smartcard PIN + PKI certificates.
  - Use Sun Ray Server and Sun VDI environment (on Sun VirtualBox or VMWare ESX)
- Sun OpenSSO / Sun Java System Access Manager
  - Multi-factor credential (PKI and Biometrics) based Single sign-on authentication to Enterprise applications.
- Sun Java System Identity Manager
  - Provisioning and De-provisioning of PIV credentials across applications.
  - Convergence of Physical and Logical Access control systems
  - Digitally Signed approvals and authorization workflows.

Smartcard/PKI Technology Providers

Integration with Sun Rays and Sun Identity Management Suite

- Daon Credential Connect
  - Integrates Physical access control systems (PACS)
    - Integrates with Sun IDM to support provisioning of credentials/roles to PACS.
- Smartcard Client Middleware
  - ActivClient 6.x (ActivIdentity), OpenSC (OpenSC.org)
    - Enables PKI authentication for Sun Ray based Desktop environments
    - Integrates Sun OpenSSO for PKI authentication enabling SSO.
    - Supports Sun Ray Windows connector and VDI environment.
    - Supports Windows Desktop SSO on Sun Rays.
    - Tested to work with FBCA PKI and DoD PKI
    - Supports Unix, Linux and Windows VDI environments
- PKI Provider
  - Entrust, Verisign, Verizon Cybertrust
  - OCSP, CRLs

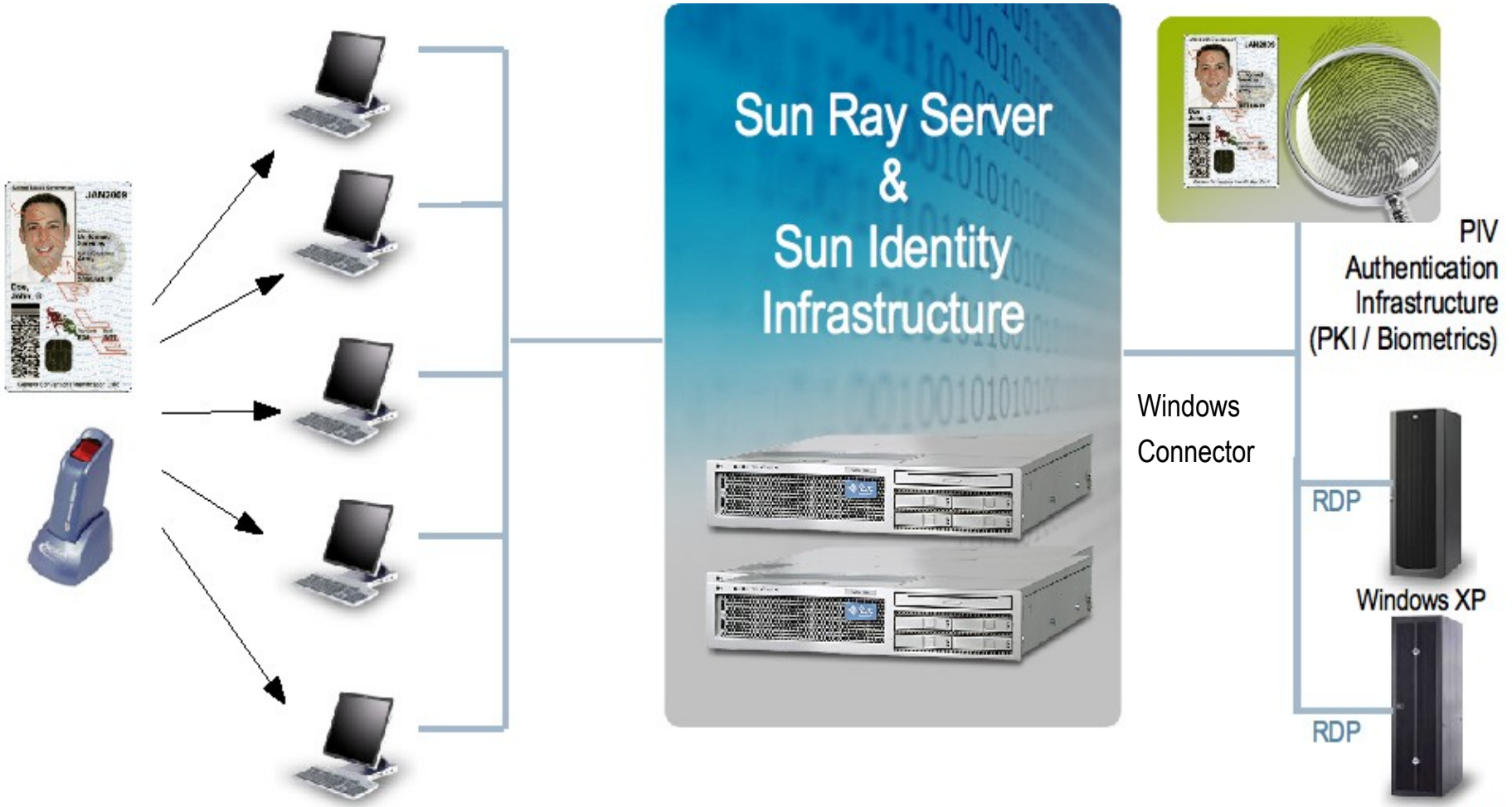
Biometric Technology Providers

Integration with Sun Rays and Sun Identity Management Suite

- Biometric Middleware
  - BioBex (Advanced Biometric Controls) and BioSP (Aware Inc.)
    - Biometric authentication middleware using samples such as Fingerprints, Iris, Facial and Hand geometry.
    - Biometric authentication for Sun Ray based Desktop environments
    - Provisioning and De-provisioning of Biometric credentials
    - Biometric authentication based Single sign-on for applications.
    - Biometrics based physical access control to restrict person access to doors, buildings and restricted areas.
    - Military-grade security with Mandatory and Discretionary access control using Solaris Trusted Extensions.
    - Match biometric samples to PIV Smart cards.
- Biometric Scanners
  - Crossmatch Verifier (Ethernet Interface)
  - SecuGen Hamster Plus (USB Interface)

Logical Architecture

PIV Credential Authentication for Sun Rays



- PKI credential status verified against FBCA PKI (via OCSP or CRLs)
- Biometric credentials matched to PIV Card or an Biometric authentication provider

Logical Deployment

PIV Credential authentication – Virtual/Remote Desktop/Application environment

PC & Thin Client users can securely access their remote desktops & applications from any location using PIV Cards.

Once PIV authenticated, the access tier establishes a display connection to the user device and a protocol connection to the back-end desktop OS and applications.

PIV Credential Authentication

Sun Rays

Access layer controls the user access and application profiles.

It maintains audit logs of user and app usage.

It provides the display engine to the user desktop.

Firewall

Secure remote access from any location

Sun Access Tier

The access tier supports standard Authentication mechanisms:

LDAPv3

Active Directory

NIS

MS Windows Domain

Firewall

Combine existing authentication and authorization mechanisms using Sun IDMS

Identity/Auth.

Each user desktop environment runs on a virtual machine located in the corporate data center.

All desktop and application communication remains in the data center.

Windows XP / 2003 Desktop Virtualization using Sun Rays and Sun VDI

ESX Virtualization

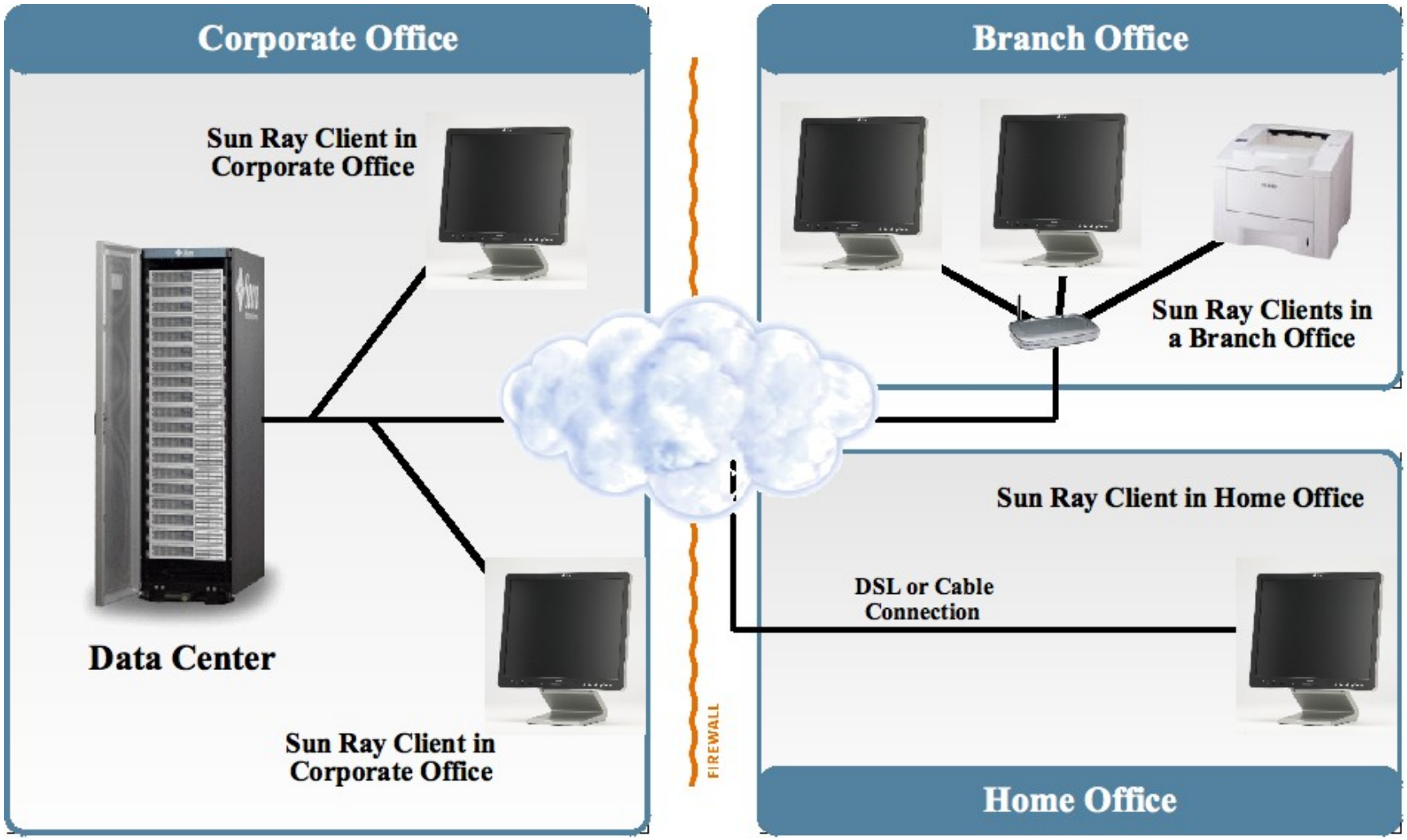
Native protocols are used to access apps.

No modification of the OS or apps required.

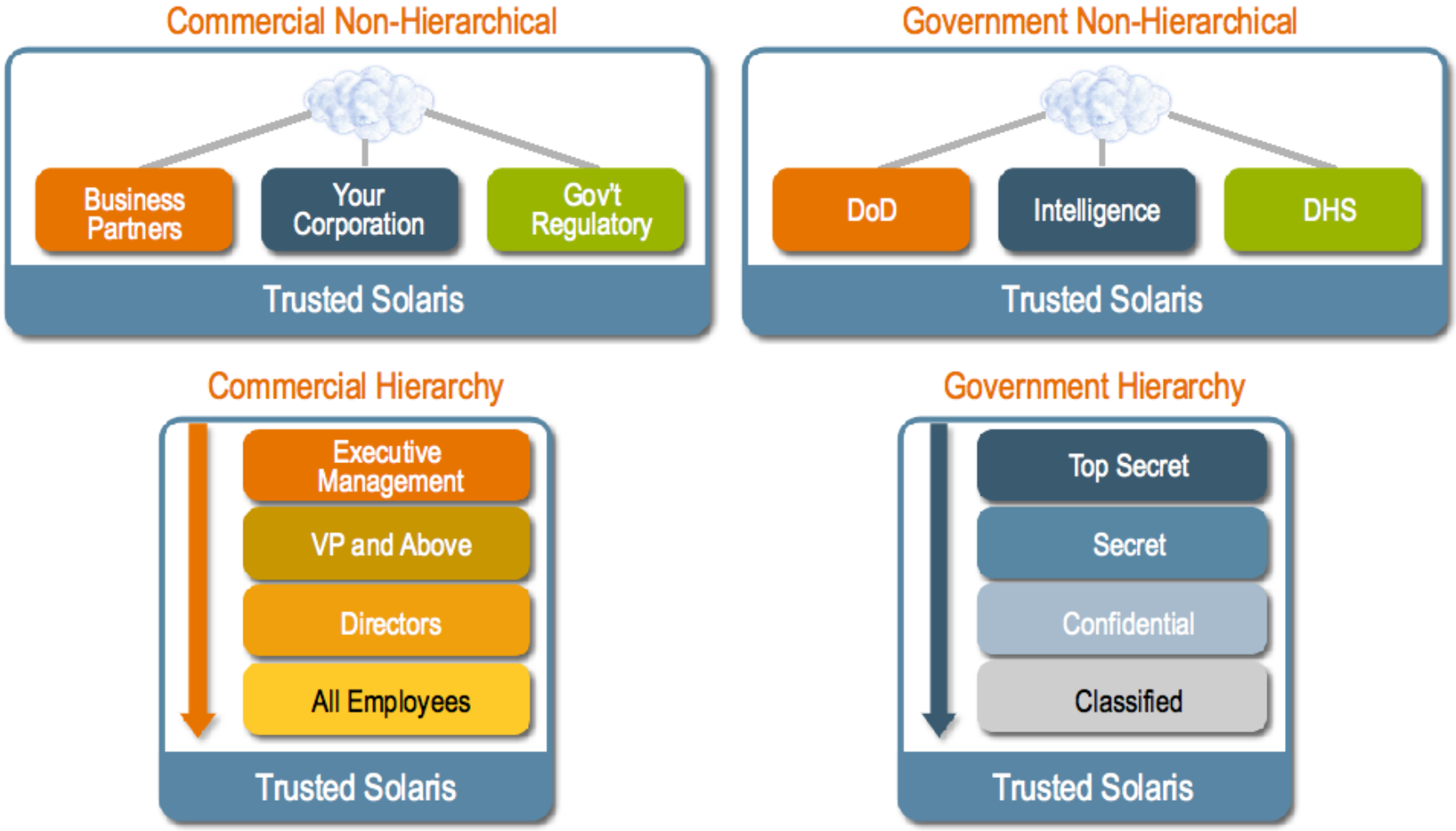
Applications

Data Center

Data and Application stay Central



Mandatory Access Control and Security Labels (Solaris TX)



Sun CMT Servers: Wire-speed Security

Sun UltraSPARC T2 offers On-chip Cryptographic Acceleration for PIV

- Sun UltraSPARC T2 offers industry-leading cryptography performance for PIV environments.
  - > On-chip Crypto threads virtually eliminates large workloads with PKI & Cryptography.
  - > Out-performs competition on SSL and Public-key crypto opertaions
    - > Over **30x** greater RSA1024 performance than 2-socket IBM p510
    - > **15.6x** better AES128 performance than off-chip crypto accelerator.
- Support common used ciphers for Public-key encryption and secure hashing functions
  - > Public-key cryptography (RSA, DSA, Diffie-Hellman, ECC)
  - > Bulk encryption (RC4, DES, 3DES, AES)
  - > Secure hash (MD5, SHA-1, SHA-256)

Q & A

Ramesh Nagappan
Sun Microsystems
ramesh.nagappan@sun.com