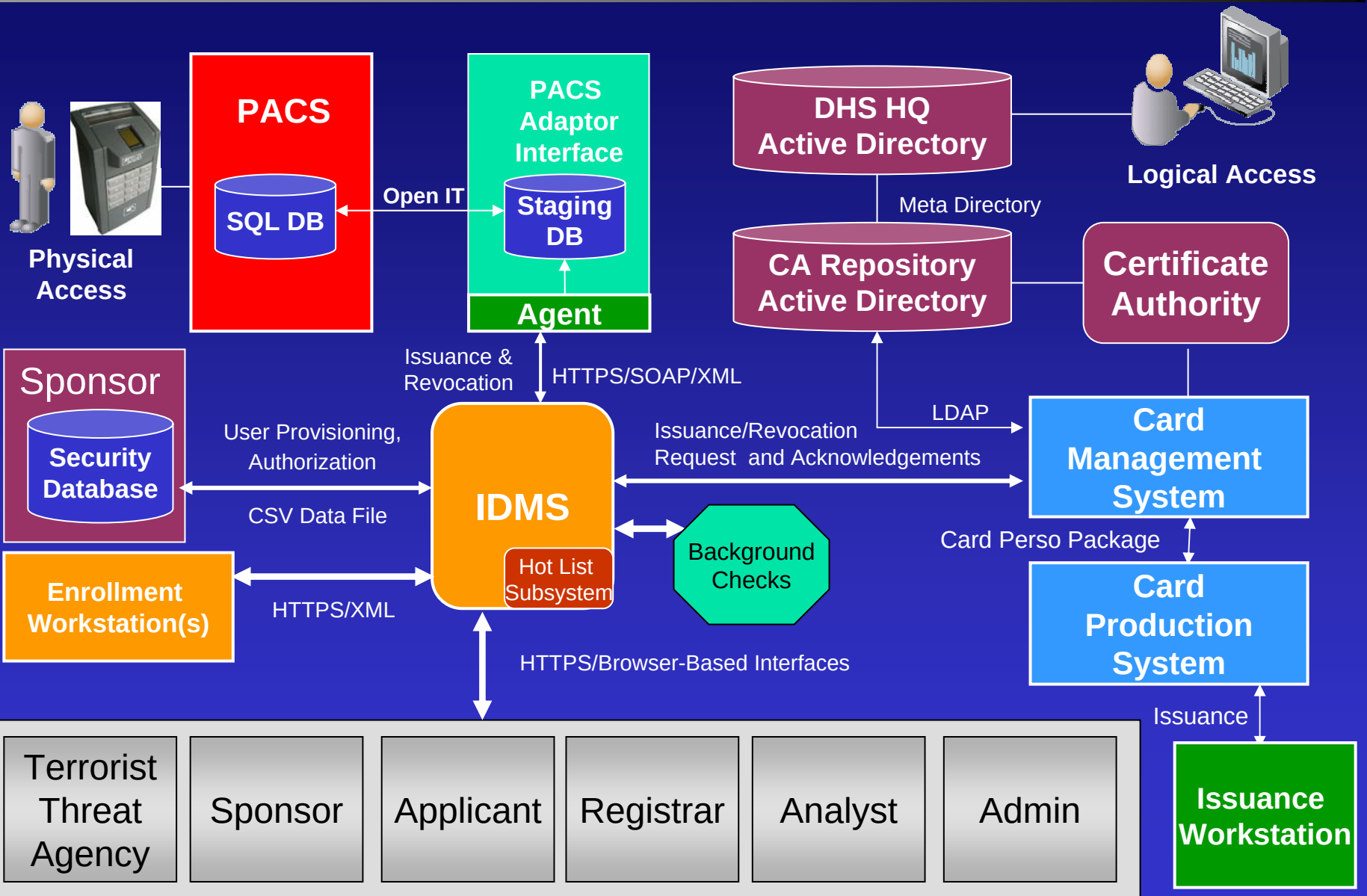
Homeland Security Presidential Directive Number 12

Integrated IDMS

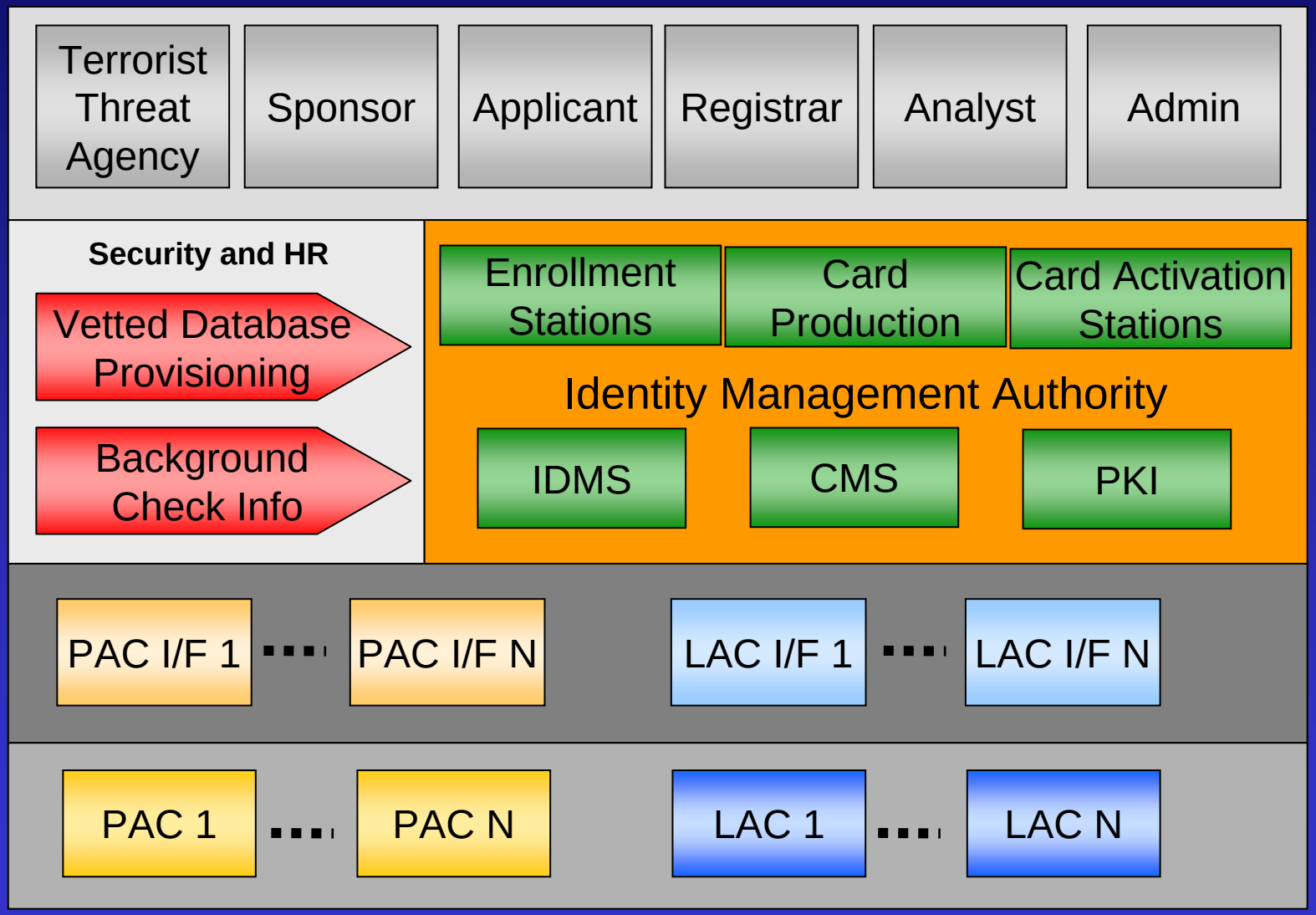
Lockheed Martin

Dave Florsek
407-306-3577

DHS FIPS 201 PIV2 Architecture



Simple Component-Based Enterprise



Lockheed Martin IDMS Scope

- Maintains overall PIV Cardholder ID data and State of PIV issuance
- Implements and enforces NIST SP 800-53 system security and privacy controls (Authorization, Auditing, Monitoring & Alerting, Data Integrity, Privacy)
- Provides Workflow, Notification, and Adjudication Management
- Provides PIV Cardholder Revocation and Hot List Management
- Provides for Standard and Ad-Hoc Reporting
- Features
  - 10 flat segmentation and conversion of biometric images to ANSI 378 Minutia and any other specified templates
  - 1:N fingerprint Credentialing Enterprise Uniqueness Check
  - CHUID, GUID and FASC-N generation
  - SF-85/86 and NAC/NACI response document capture
  - Sponsor Provisioning Interface – IDMS provisioning and go/no-go adjudication decision interface
  - CMS Card Request and success/failure notification interface
  - PACS to IDMS and IDMS to IDMS Interfaces

Lockheed Martin IDMS Key Technologies

- IDMS is wholly compliant to all current HSPD-12 requirements
- All interfaces use HTTPS
- All privacy data is explicitly encrypted
- Sponsor and Enrollment messages are stored in original encrypted and signed form
- Sponsors and other major entities are explicitly assigned using Entity Registration with complete auditability and tracking including certificate provisioning
- IDMS is designed for large-scale operation to provide built-in scalability
- IDMS is built over J2EE platform using a Service-Oriented Architecture

Chain-of-Trust

First link in chain Crucial to secure process

Identity Management Authority

Sensitive Info & Docs

HTTPS Transport Communication

App CSV

Conf. CSV

Web Portal

Enrollment Package

Resolution Info & Docs

Web Portal

Sponsor Vetting

Sponsor

Pre-Enrollment

Enrollment

Registrar Adjudication

Credential Issuance

Audit

Security Database

Application

NAC/NACI Request

Applicant Job Requirements

Sponsor Credential

Update Information

Trusted Agent Credential

Registrar Credential

Issuer Credential

Auditor Credential

Signed PIV Request

I-9 and Identity Docs

Bio Data

Background Check Results

Anomaly Resolution Docs

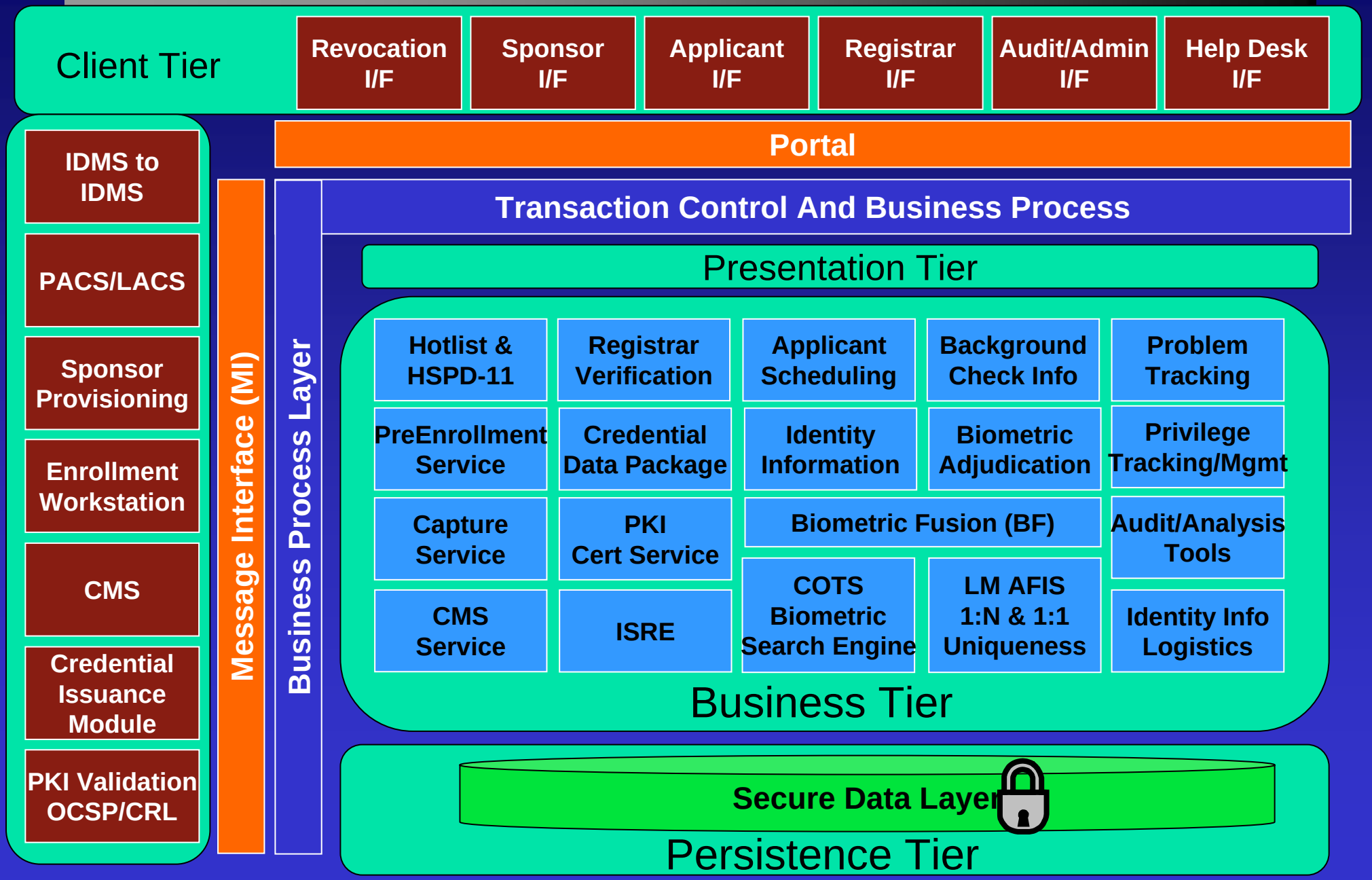
1:1 Biometric Check

Credential Activation

New Cred

Trust preserved through the entire path

Lockheed Martin IDMS Enterprise Model



Major Interfaces

- User Interfaces
  - Revocation
  - Sponsor
  - Applicant
  - Registrar
  - Issuer
  - Admin
  - Auditor
  - Help Desk
- System Interfaces
  - IDMS to IDMS
  - PACS
  - LACS
  - Sponsor Data
  - Enrollment
  - Background Check
  - CMS
  - Card Issuance
  - PKI/OCSP/CRL

IDMS must securely interface all roles and systems

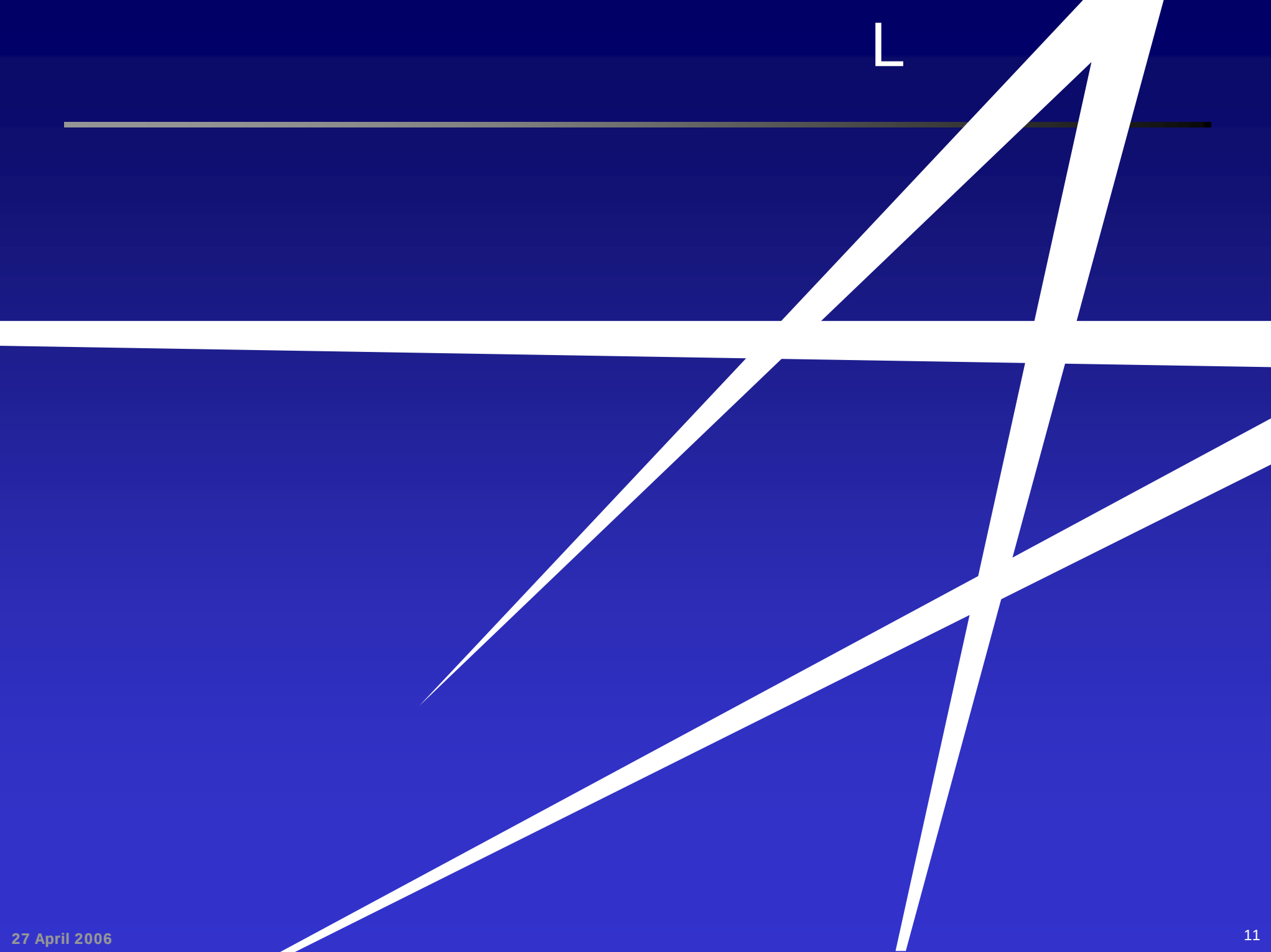
FAQs

- How does the first Sponsor or Registrar get a card?
- What if the Applicant has poor quality prints?
- How do I get interoperability across PACS & LACS?
- How do I get the highest security and interoperability across a real enterprise?
- How do I adjudicate thousands of Applicants in a reasonable amount of time?
- How do I enroll in a cost-effective manner across the entire country or world?
- How can I define a reasonable Sponsor data model?
- What do I use instead of an SSN?

Your IDMS Integrator Should Answer These Questions

Conclusion – What needs to be done

- Common CONOPS
- Published policy standards from each Agency
  - Driving down details of data usage/needs
  - Clearance levels
- Published Interface Control Documents for each component
- Memorandum of Understanding for data sharing


L