

Interagency Advisory Board

Meeting Agenda, Wednesday, December 7, 2011

1. **Opening Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **FIPS 201-2 Goes Mobile** (*Bill MacGregor, NIST*)
3. **Logon to Google Apps Using NASA Issued PIV** (*Tim Baldrige, NASA, IAB Chair*)
4. **Implementing PKE for JPAS** (*Maxwell Funk and Autumn Crawford-Grijalva, DoD*)
5. **Provisioning PACS using the GAMS** (*Hiddemen, Brad, GSA*)
6. **Closing Remarks** (*Mr. Tim Baldrige, IAB Chair*)



OCIO

GSA Access Management System (GAMS)

PACS Provisioning Overview

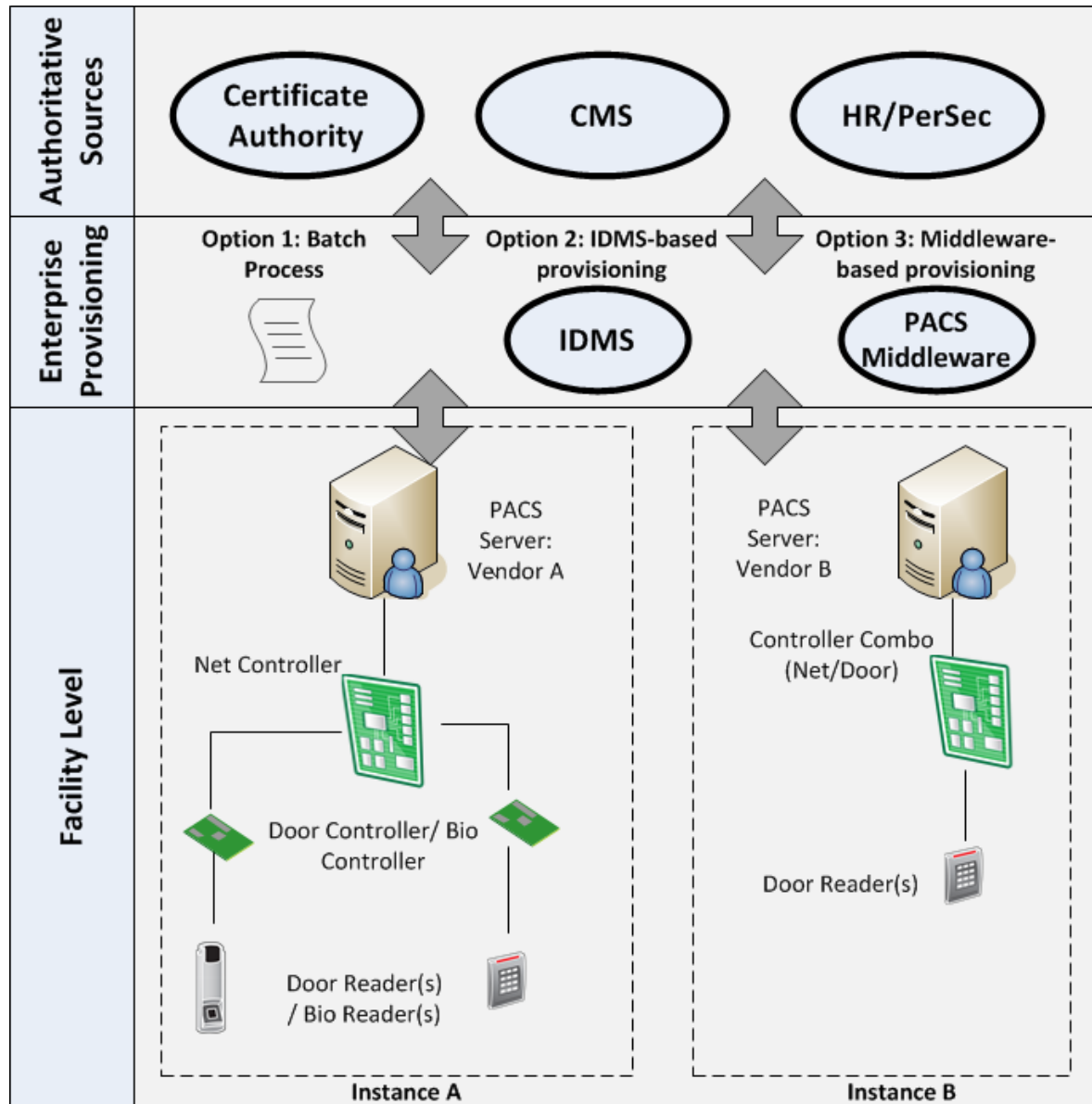
Identity, Credential and Access Management (ICAM) Division

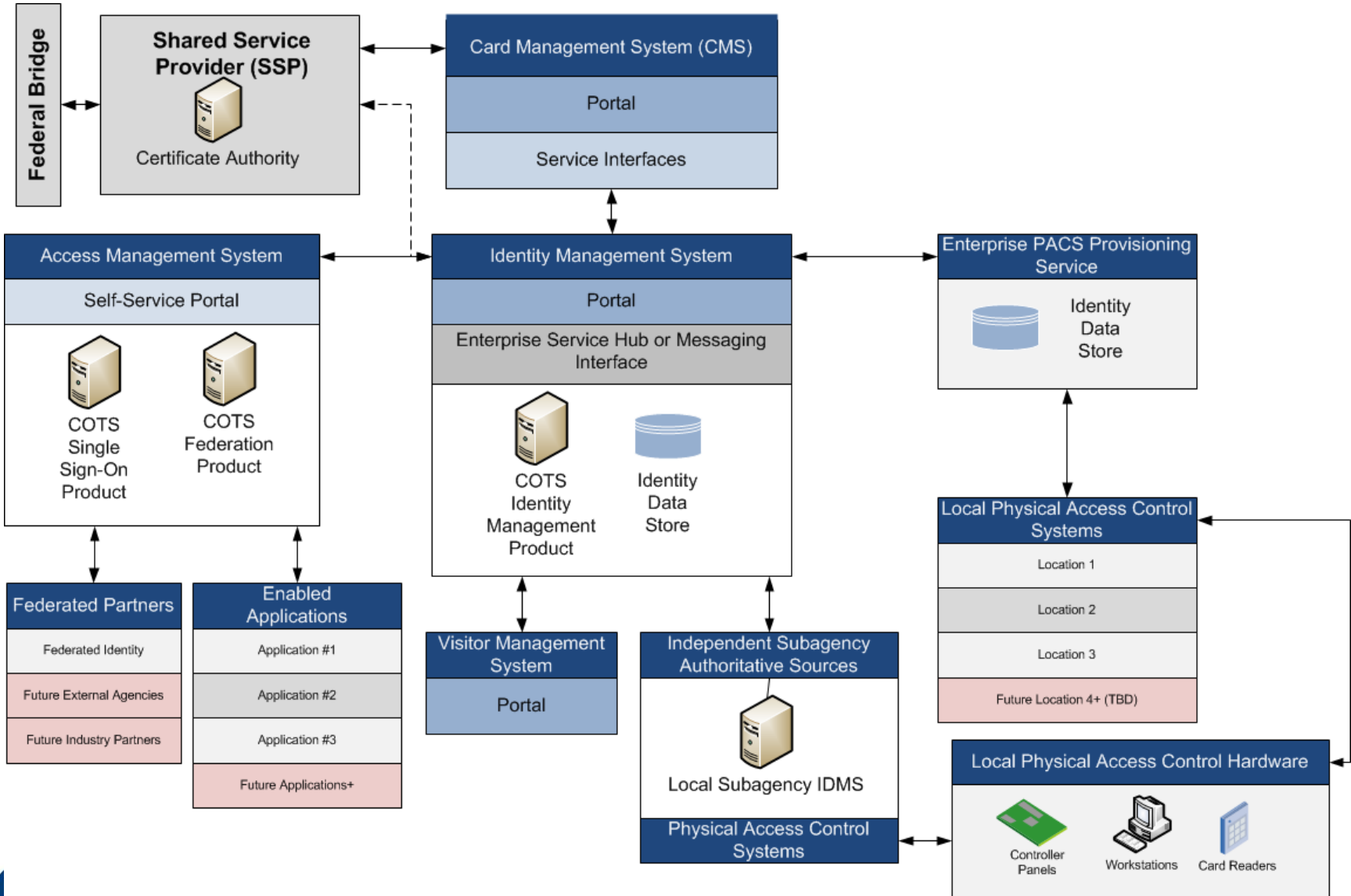
December 7, 2011



- **Overview of PACS Provisioning Options**
- **Architectural Example: PACS Middleware Provisioning**
- **Implementation Considerations**
- **Questions**

PACS Provisioning Overview





Considerations for PACS Provisioning

- Understanding Scope: In the short term, custom IDMS connectors may be feasible but may not scale with a growing enterprise or provide the modularized additional functionality of a COTS PACS middleware solution.
- Provisioning Versus Policy: Most PACS system owners associate identity provisioning with access rights (e.g. front door) which is a common stakeholder misconception

Considerations for Visitor Management

- Licensing: Registering external users creates additional costs for systems using a per user/seat license model. This may impact the licensing of existing PACS and/or LACS systems.
- CRL Checking: Additional CRLs must be added for each external user group.
- Lack of Internal Trust Policies: Before a credential can be trusted there must be an internal trust process created for accepting credential service provider issued third-party credentials.

Considerations for PIV-I Acceptance

- Lack of FASC-N: Many existing Federal PACS and LACS implementations are specific to the FASC-N identifier on PIV cards. Acceptance of PIV-I would be dependent upon upgrades/enhancements to accept either FASC-N or the PIV-I's UUID.

