SCA Spring 2006 Conference GSC-IAB's Backend Authentication Scheme Work Group (BAS WG) Brief

19 April 2006

Tim Baldridge, CISSP, MCSE
BAS WG co-chair

IAB BAS WG Task

Challenge #1: Other Federal Agency Visitors

- FIPS 201 (section 6.2) requires card issuers to provide the capability for credentials to be authenticated by other Federal Agencies

Challenge #2: Electronic Way to Review NACI Status of Visitors

- OMB M-05-06 and FIPS 201-1 Identity Credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable form identity credentials issued to individuals who have a completed investigation.
- NACI status may indicate incomplete at PIV issuance
- How is visitor NACI complete status verified

Guiding Principles

- **Approach to Challenge of Authenticating Other Federal Agencies' Credentials must:**
  - Establish a Uniform way for PIV issuance backends (e.g. IdMS) to communicate with other PIV issuance backends to determine if a credential is **valid** and **authentic**
  - Attempt to use web-base tools to the maximum extent possible
  - Attempt to incorporate additional authentication mechanisms like PKI, biometrics or photo.

- **Approach to NACI Challenge must include:**
  - Systems and token interoperability
  - Credential cross recognition
  - Open architecture design
  - Existing infrastructure investments
  - Scalability and ability to include functional options beyond basic functionality

Credential Qualifications

- Not Specified in HSPD-12 or FIPS 201
- Determination of Personnel Qualifications
  - PIV II Cards with Biometric verification determine minimum standard validation (NAC-I) for Federal Personnel
  - Many Agencies have a demonstrated requirement for additional information from the PCI for a specific visitor to determine suitability of the visitor for a requested access

Focus of BAS WG Efforts

BAS WG has identified four areas to this challenge:

1. Ability to Authenticate and validate PIV Credentials of Visitors
2. Ability to take information obtained from Authenticating Visitors or backend PIV infrastructure and registering this information within the Local Physical Access Systems
3. Ability to verify and authorize PIV Cardholders during daily use within the Local Physical Access System
4. Ability for Backend PIV infrastructure to make available information on changes in card validity (e.g. terminations, lost/stolen, ect..) of PIV cardholders

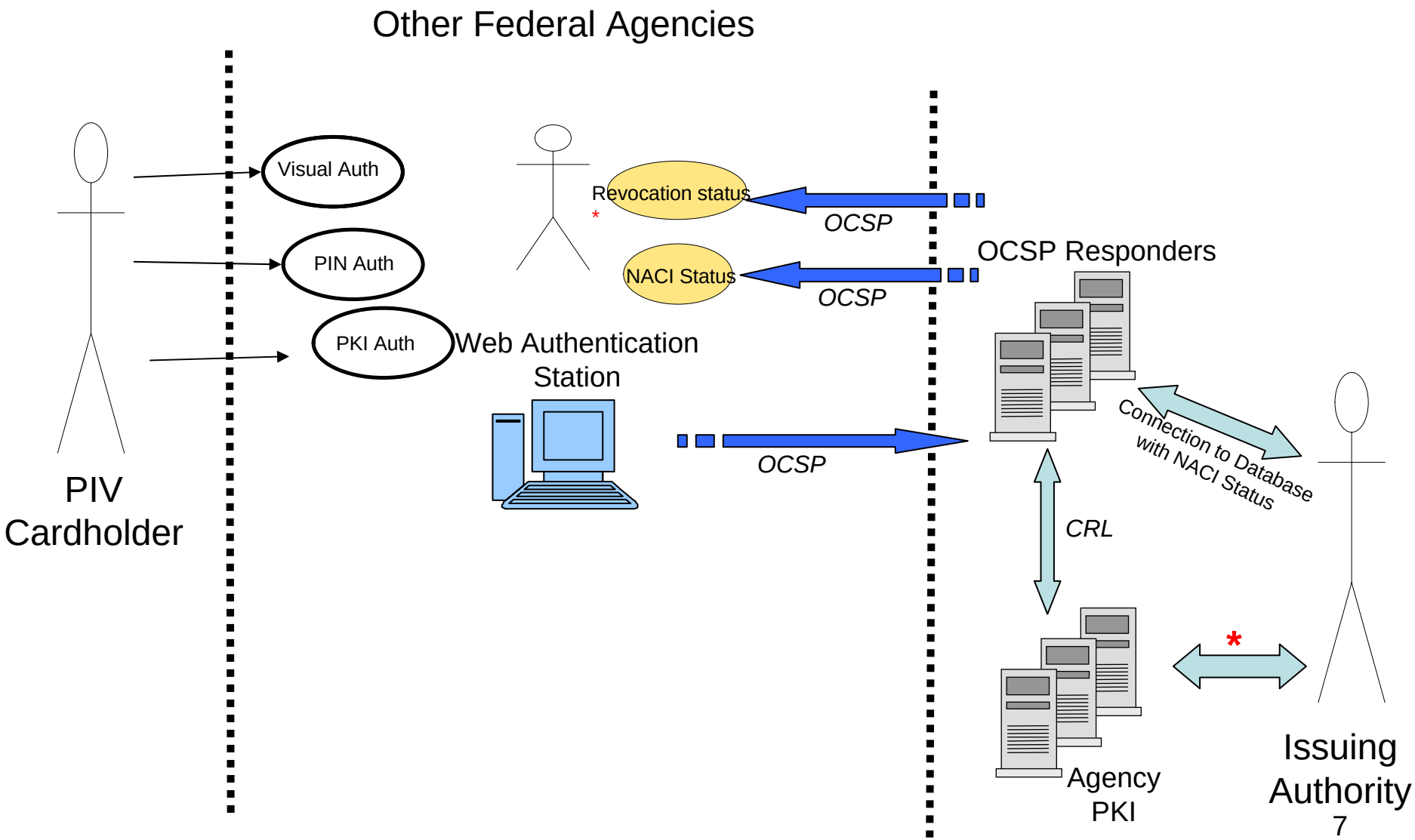
The Group must minimally address #1 and #4

Approaches

- Government members of the BAS WG detailed two approaches
  1. Gateway Approach (proposed by DoD)
     - Signed communications or Signed objects
  2. OCSP Approach (proposed by NIST)
     - Signed objects

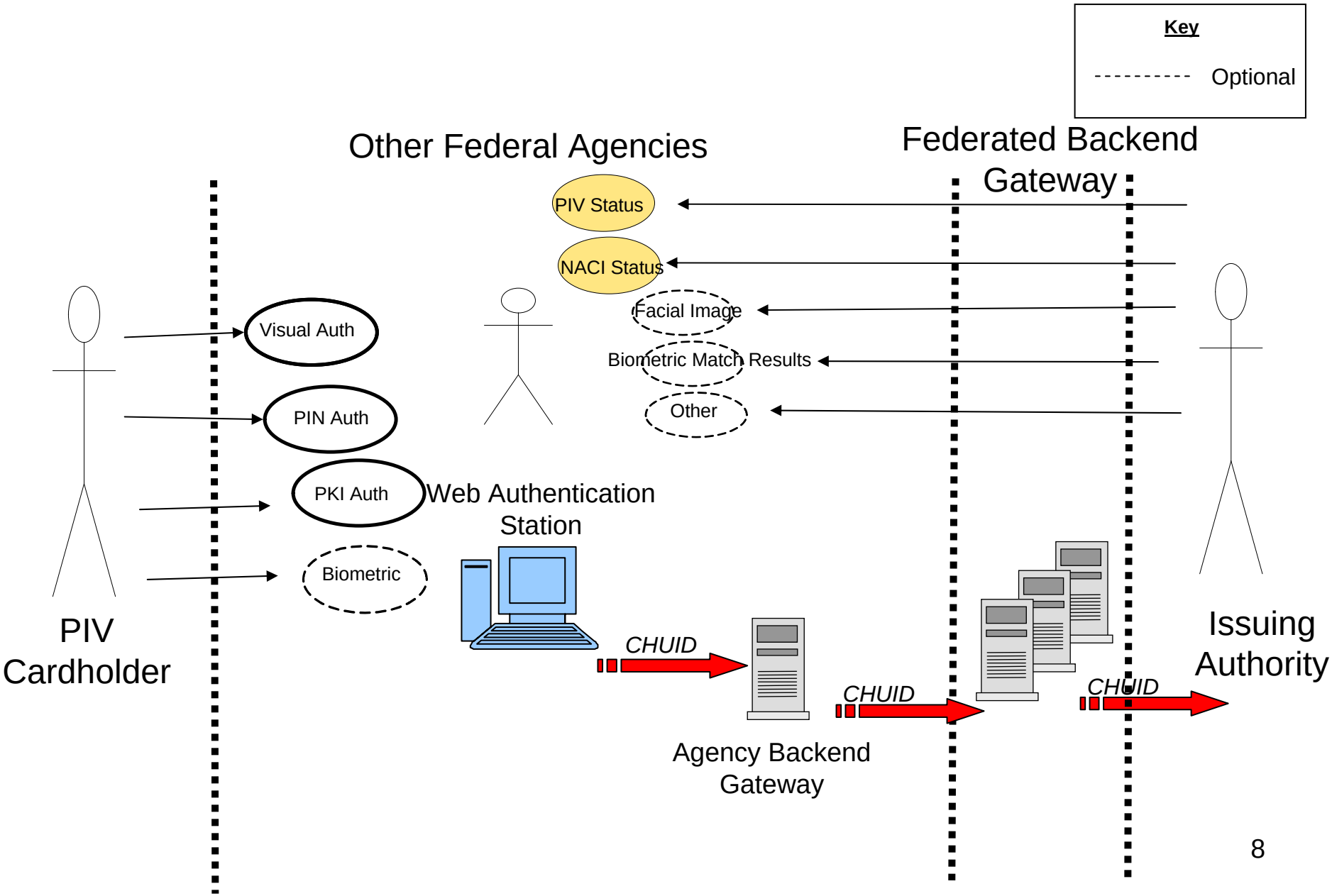
- The next series of slides outlines the use case scenarios for each proposal to meet “focus areas” #1 and #4.

PIV Backend Authentication Scheme—FD #1 (OCSP Approach)

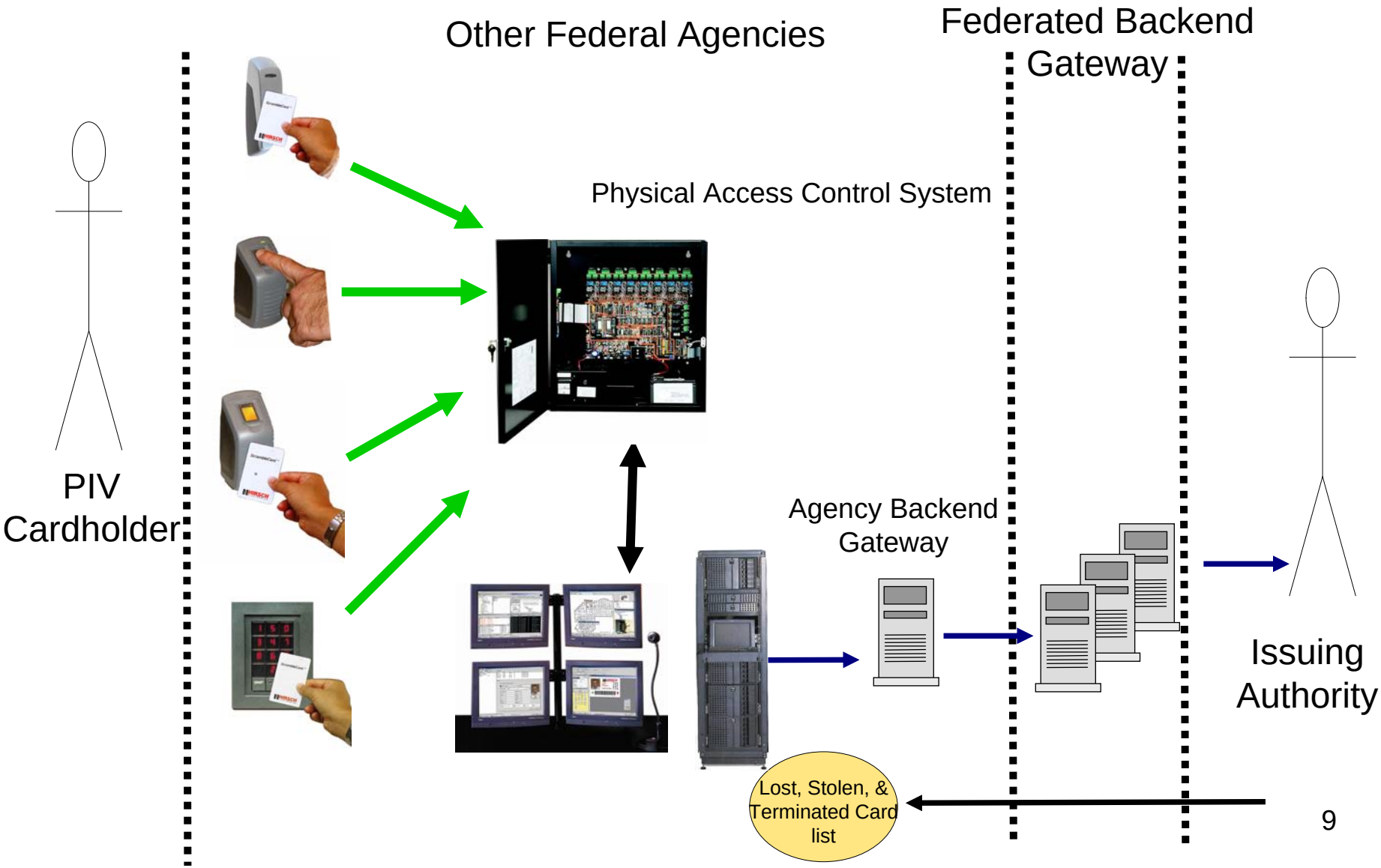


*Assumes the PIV issuing authority is link to Agencies PKI in virtual real-time.

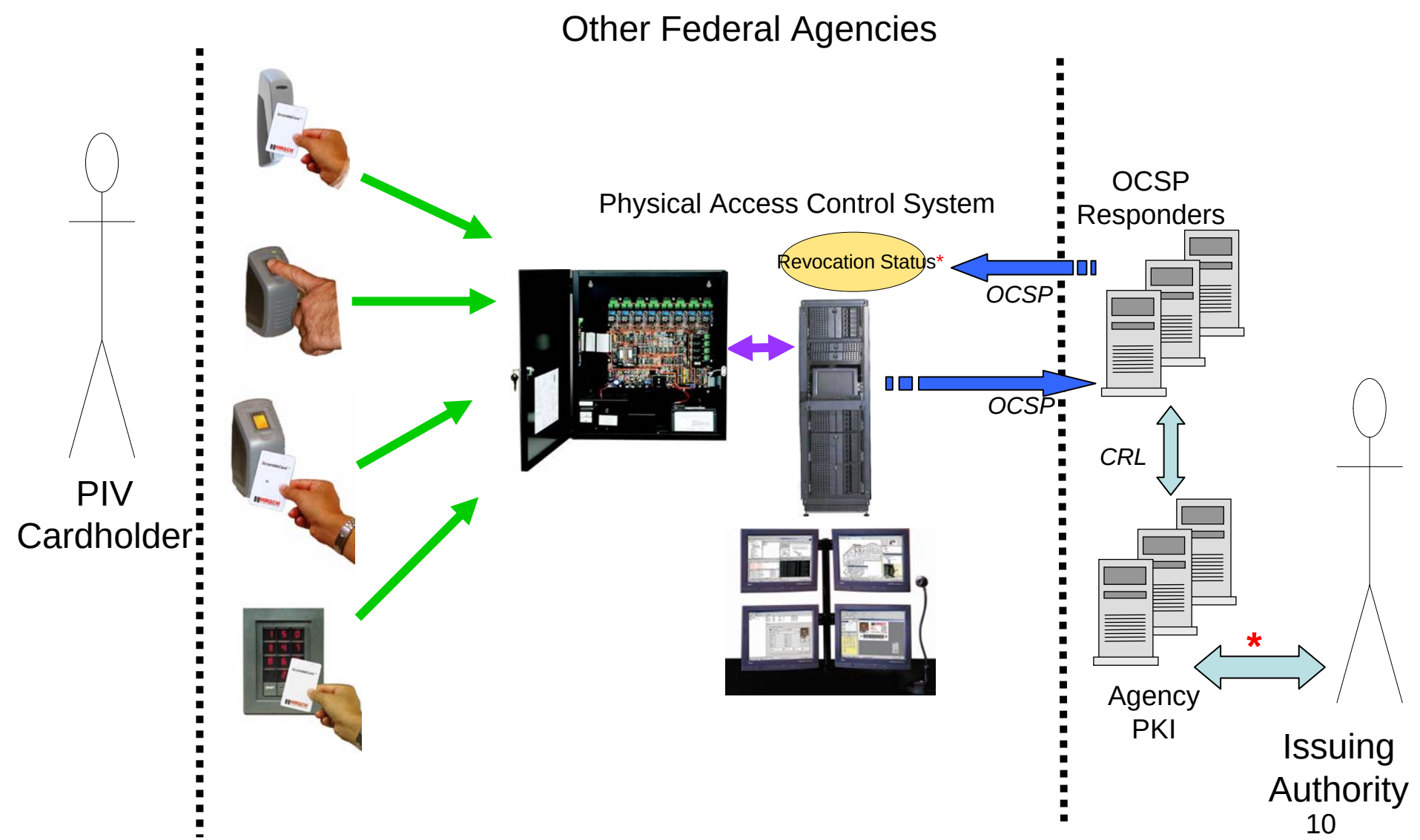
PIV Backend Authentication Scheme—FD #1 (Gateway Approach)



PIV Backend Authentication Scheme—FD #4 (Gateway Approach)



PIV Backend Authentication Scheme—FD #4 (OCSP Approach)



*Assumes the PIV issuing authority is link to Agencies PKI in virtual real-time.

Potential Challenge

- Weighing privacy with implementation approaches
  - Technically some pieces of the two approaches are inherently public (e.g. available to whoever requests or views the service)
    - Raises a question on whether the NACI status information should be made publicly available
    - If not, then what are the best mechanisms to protect against unintended, unauthorized disclosure

Status

- Industry Review (began Tuesday, Feb 28)
  - Conducted conference call with approximately 35-45 Industry participants
  - The Government members work was presented
  - Industry provide ONLY 3 sets of comments on proposed approaches

- Final Recommendations (following April IAB)
  - Government members will review Industry recommendations to decide which approach to recommend to the full IAB.

Back up

IAB BAS WG membership

BAS WG membership include representatives from:

- DOI
- NASA
- NIST
- DOT
- DHS
- DOS
- DOD
- FAA
- and Industry