QUANTUMSECURE

Next Generation CIV Credentials for Department of Energy National Labs

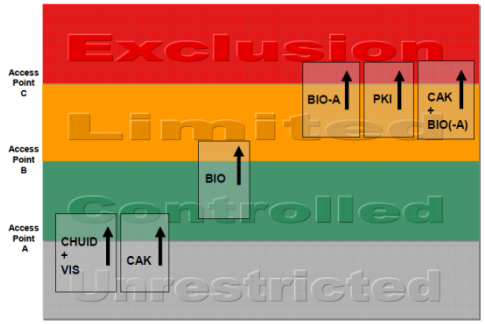
Interoperability with PIV/PIV-I Infrastructure

Smart Card Alliance Government Summit

October 2013

DOE Compliance Environment

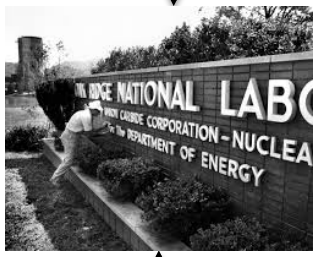
NIST SP 800-116



DOE Directives:

DOE M 470.4-2A (physical protection)
DOE M 472.1-1A (personnel security program)
DOE N 206.4 (personal identity verification),
DOE O 142.3 & DOE O 142.1 (classified and unclassified foreign visitor's identity management)
Plus DOE P 470.1, DOE M 470.4-2A, DOE M 471.2-3B, etc.

FISMA



HSPD-12

ICAM Identity, Credential, & Access Management

EXECUTIVE OFFICE OF THE PRE
OFFICE OF MANAGEMENT AND BU
WASHINGTON, D.C. 20503

THE DIRECTOR

February 3, 2011

M-11-11

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors

OMB M-11-11

- PIV/CAC interoperability
- FICAM Version 2 Alignment
- Use the card for access

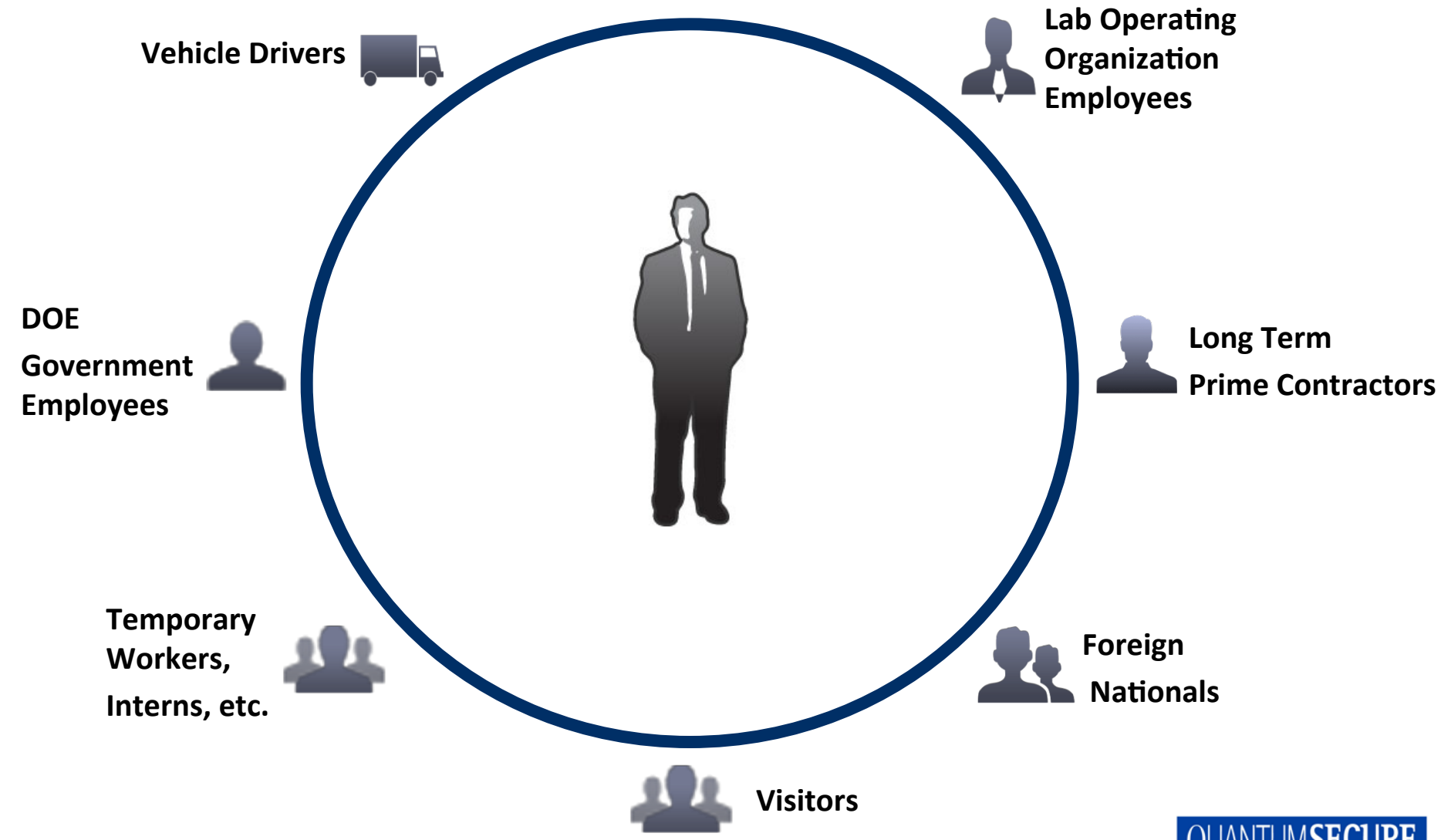
Department of Energy (DOE) Federated Identity, Credential, and Access Management (ICAM) Framework Version 1.0

U.S. DEPARTMENT OF ENERGY

Federated PACS Guidance

QUANTUMSECURE

DOE National Labs Identity Types



QUANTUMSECURE

FICAM is Reshaping DOE Labs Legacy Environment

- Legacy Mag Strip or Prox cards are largely still in use today for physical access
- Department of Energy FICAM Framework now mandates use for PIV for logical and physical access.
- Depending on the Lab, between 30% and 70% of personnel now have PIV cards, provided by DOE
- Labs are engaged in upgrading infrastructure for both logical and physical access systems to accept PIV cards for use
- Which leaves the question of the non-PIV population – what to do?

Options to Close the Gap

Options	Pros	Cons
Option 1: Maintain legacy prox or mag stripe cards for physical security and User login/password for logical access	1. Don't rock the boat 2. Legacy cards are cheap	1. Cost of maintain two separate infrastructures (PIV and non-PIV) 2. Increased security risk
Option 2: Issue PIV-I to everyone else	1. Achieve FICAM Framework Alignment 2. Increase security	Cost of PIV-I is significant
Option 3: Issue CIV to everyone else	3. CIV cards are cheap	CIV is not federated (but does that matter?)

QUANTUMSECURE

Credential Comparison

Credential	Issuer	Card Type	Card Payload	Certificate Provider	Trust Model	Comments	Cost
PIV 	Federal	Smart Card Mifare Chip	PIV (Person, Bio, Picture, Certificates)	CA cross-certified with the FBCA	Global PKI (Federated) NACI Background Check	Defined by FIPS 201-2 FASC-N	$$$$$
PIV-I 	Non-Federal	Smart Card Mifare Chip	PIV (Person, Bio, Picture, Certificates)	CA cross-certified with the FBCA	Global PKI (Federated)	Defined by FIPS 201-2 UUID	$$$$
CIV Smart *** 	Federal & Non-Federal	Smart Card Mifare Chip	PIV-Like (Person, Bio, Picture, Certificates)	Local/Hosted CA	Local PKI (within Agency Domain Only)	Defined by Smart Card Alliance UUID	$$
Legacy 	Federal & Non-Federal	PVC Card (Prox, Magstripe, Other,)	(Person, Picture)	None	Local Site	Legacy Technologies Mag Stripe Wiegen	$
Paper 	Federal & Non-Federal	Self-Expiry Paper Pass	(Person)	None	Local Site	Paper or Plastic flash pass	0

***** The Commercial Identity Verification (CIV) Credential–Leveraging FIPS 201 and the PIV Specifications**

http://www.smartcardalliance.org/pages/publications-the-commercial-identity-verification-civ-credential-leveraging-fips-201-and-the-piv-specifications

QUANTUMSECURE

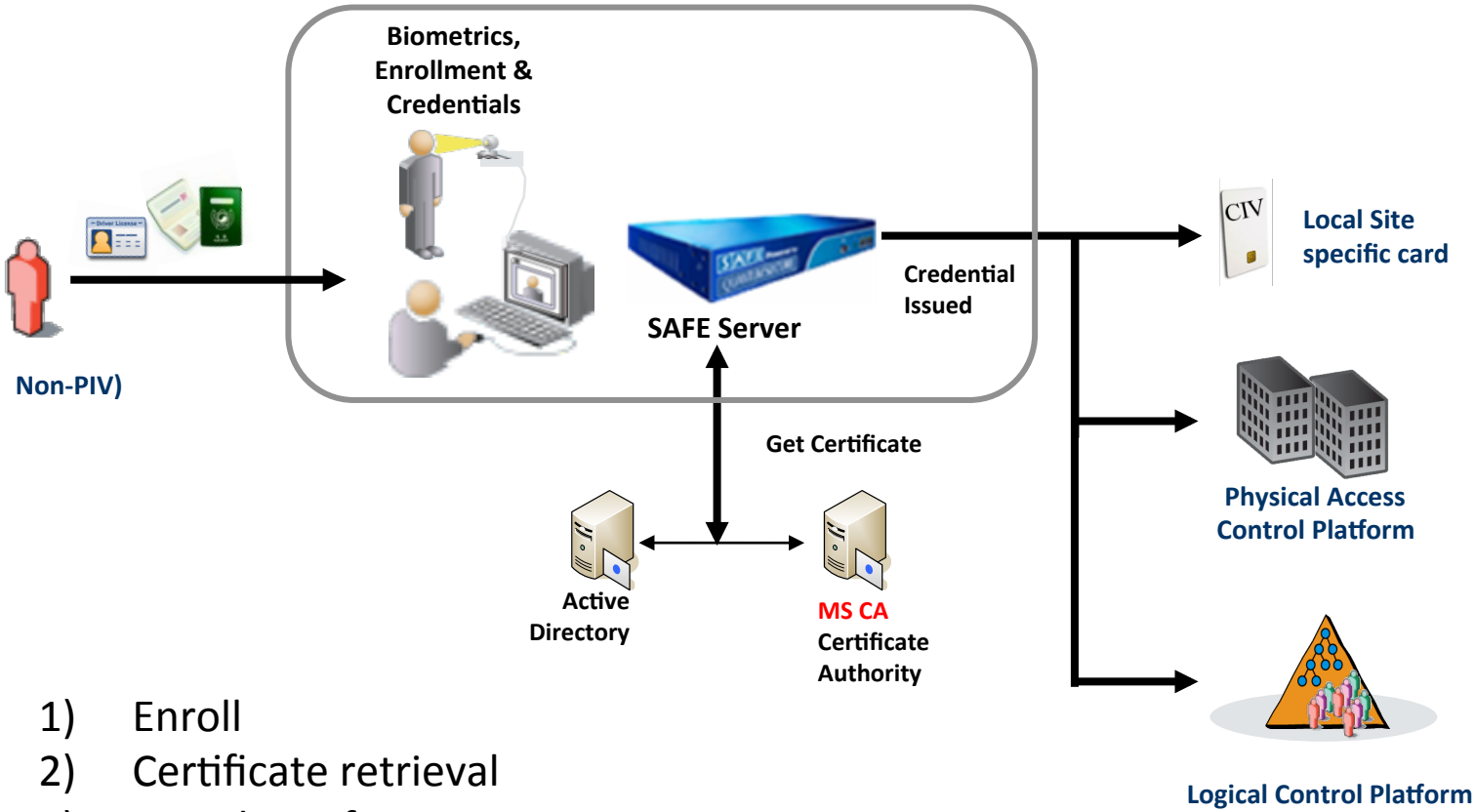
Badging Reality for DOE Sites

Identity	Physical Access	Logical Access	As Is Card Type	Target Card Type	Cost Implication
Battelle Employee	Yes	yes	Legacy	CIV	Battelle pays
Federal (DOE) Employee	yes	varies	PIV	PIV	DOE pays
Numerous Prime Contractors	yes	varies	Legacy	PIV-I CIV	Contractor pays
Foreign National Researchers	yes	yes	PIV	CIV	Battelle pays
Foreign Visitors	escort	no	Plastic ID	Paper or CIV	Battelle pays
US Citizen Visitors	escort	no	Plastic ID	Paper or CIV	Battelle pays

***** Example based on Oak Ridge National Labs

QUANTUMSECURE

Workflow for Issuance of LSSO Smart Card



1) Enroll
2) Certificate retrieval
3) Encoding of CIV
4) Provision CIV to Relying Party Systems

QUANTUMSECURE

Key Benefits Realized with CIV Cards

Cost: Reduces the cost of managing multiple credentials esp. high-priced security tokens by using CIV cards for logical access

Flexibility: Ability to issue card based on business need – for logical & physical access

Support Lifecycle Changes: Identity lifecycle, which might include revocation, reissuance/replacement, re-enrollment, expiration, PIN reset, suspension, re-instatement, etc.

Superior Compliance: Enforce compliance through real-time synchronization of user status in access control systems.

QUANTUMSECURE