PKI and FICAM Overview and Outlook

CertiPath

Stepping Stones

2001 FPKIPA Established

- Federal Bridge CA established

2003 E-Authentication Program Established

- M-04-04 *E-Authentication Guidance for Federal Agencies* published

2004 Homeland Security Presidential Directive 12 published

- Federal Common Policy Framework Root CA is established
- SP 800-63 *Electronic Authentication Guideline* published

2005 FIPS 201 *Personal Identity Verification of Federal Employees and Contractors* Published

- PIV Card deployment begins

2009 ICAMSC established by Federal CIO Council

- Federal Identity Management Segment Architecture Published
- National Strategy for Trusted Identities in Cyberspace (NSTIC) launched

2017 Establish Federal TLS Root

- Following CAB Forum criteria for publicly trusted roots

CertiPath

Enabling Policy and Guidance

The E-Gov Act 0f 2002

The Government Paperwork Elimination Act 0f 1998

The Implementing Guidance: OMB M-04-04 December 16, 2003

The Implementing Guidance: OMB M-00-10 April 25, 2000

Federal Bridge Model Policy

Federal PKI Common Policy Framework

The Mandate: HSPD-12 August 27, 2004

The Technical Spec: SP 800-63 June 2004

The Standard: FIPS-201 February 25, 2005

The Implementing Guidance: OMB M-05-05 December 20, 2004

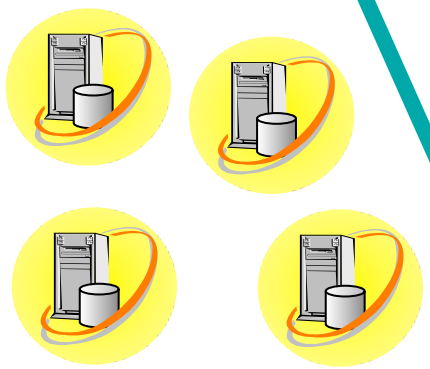
SP 800-63-3 TBA - 2017

The Implementing Guidance: OMB M-05-24 August 5, 2005 OMB M-11-11 February 3, 2011

Special Publications Technical Specs.

CertiPath

Evolution of Federal PKI



Individual Agencies implemented Enterprise PKI

- Individual investments
- No standardization
- No interoperability
- No trust between organizations
- Limited number of agencies making investment

BEFORE 2002

EVOLUTION

Federal Common Policy CA

2003
Trust extended to State of Illinois

2002
"Legacy" Agencies achieve interoperability & mutual trust facilitated by FBCA

Federal Bridge CA

2006
Aerospace-Defense & Bio-Pharma industries adopt Bridge model & establish trust with FBCA

2004
Shared Service Providers make PKI economical & available to Federal agencies for PIV credentials (HSPD-12)

Federal Agencies

2009
Commercial Shared Services make PKI economical & available to State, Local, Tribal government and Business community for PIV-Interoperable credentials

2017
Federal TLS Root in development in response to CAB Forum requirements

CertiPath

ICAM

- ICAM represents the intersection of digital identities, credentials, and access control into one comprehensive approach.

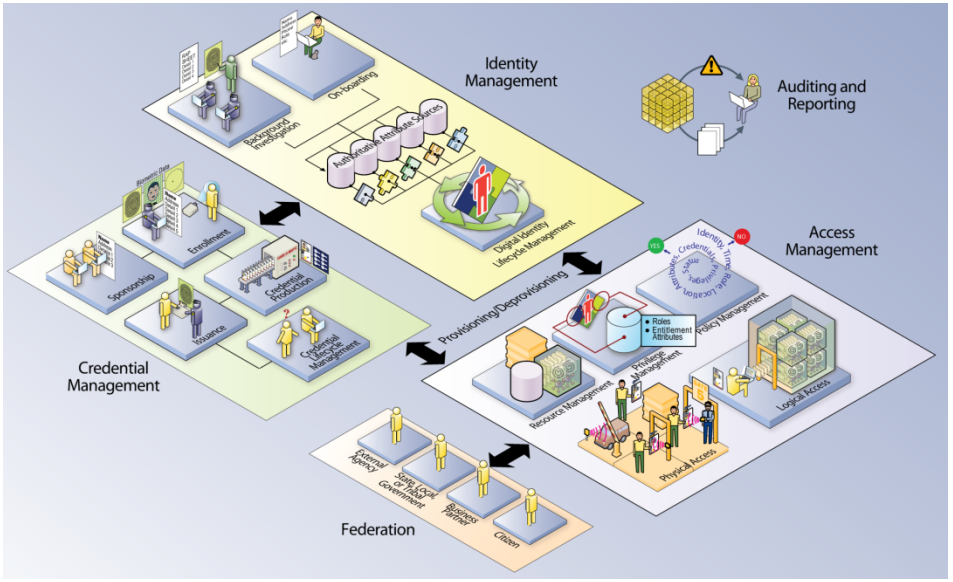
  Consolidates 3 Programs:
  - E-Authentication
  - Federal PKI
  - HSPD-12

  Streamlines government-wide activities

  Minimizes duplication of effort

  Breaks down stovepipes

  Key enabler for National Strategy for Trusted Identities in Cyberspace



CertiPath

ICAM Scope

Persons
Non-Persons

4 Levels of Identity Assurance
(No confidence through full confidence)

Enable Trust and Interoperability

Internal to the Federal Community (IEE)	• Intra-Agency • Inter-Agency
With Other Governments (G2G)	• State • Local • Tribal • Allied Partners
With External Organizations (G2B)	• Industry • Financial Institutions • Healthcare Providers
With the American People (G2C)	• Taxpayers • Grant Recipients • Medicare/Medicaid Beneficiaries

Credential Types

- **PIV Credentials**
- **PIV-Interoperable Credentials**
- **Open Solutions**
  - OpenID
  - iCard
  - SAML
  - WSFed
  - Etc.

Logical Access
Physical Access

CertiPath

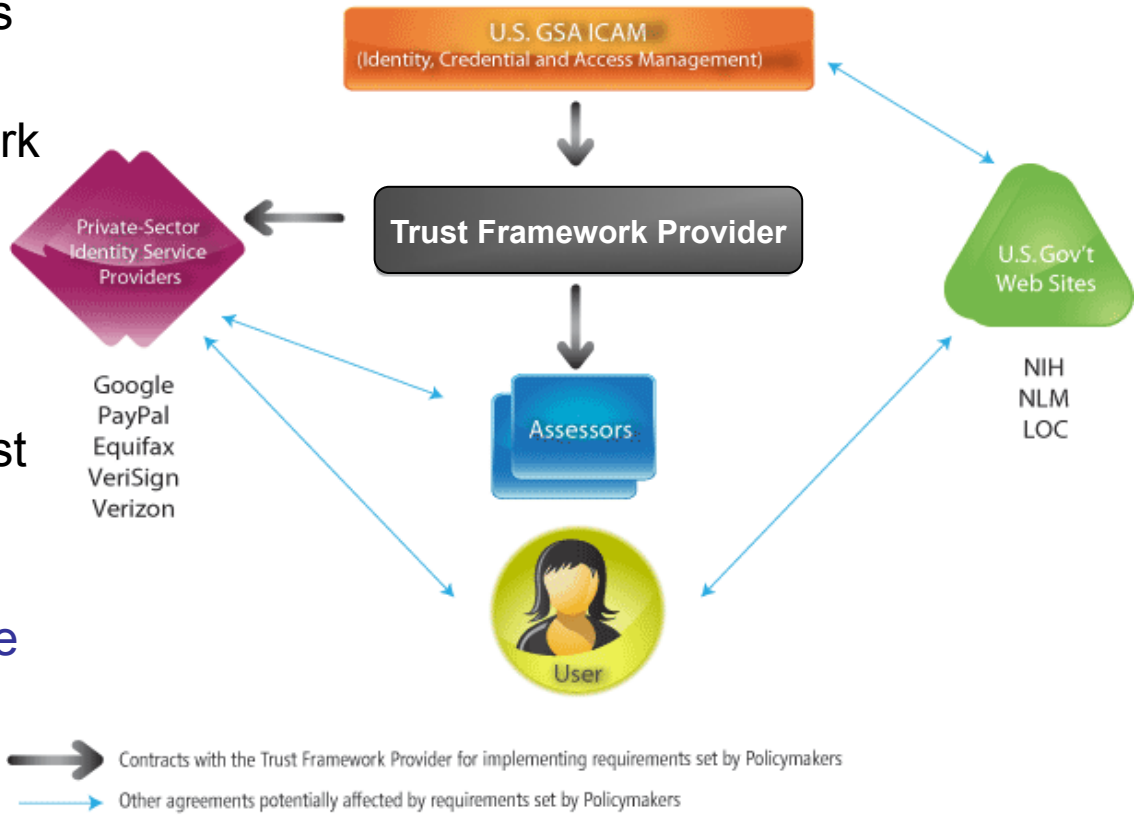
ICAM Key Activities

- Continuing growth of PIV-based Identity Assurance in the Federal enterprise
- Administering the Federal PKI
- Coordinating interagency efforts to meet agency mission needs
- Trust Framework Providers and Scheme Adoption
  - Non-cryptographic solutions at lower levels of assurance
  - Industry self-regulation with government recognition
  - Working with Open Solutions to enable open government
- Revamping FICAM Architecture implementation guidance = Playbooks

Trust Frameworks: Open Solutions for Open Government

The ICAMSC:

- Establishes Federal Profiles for Open identity solutions
- Established Trust Framework Provider Requirements
- Worked the CIO Privacy Committee to establish Privacy Principles
- Reviews and Approves Trust Frameworks:
  - Kantara
  - Open Identity Exchange
  - InCommon



Graphic Courtesy of Open Identity Exchange

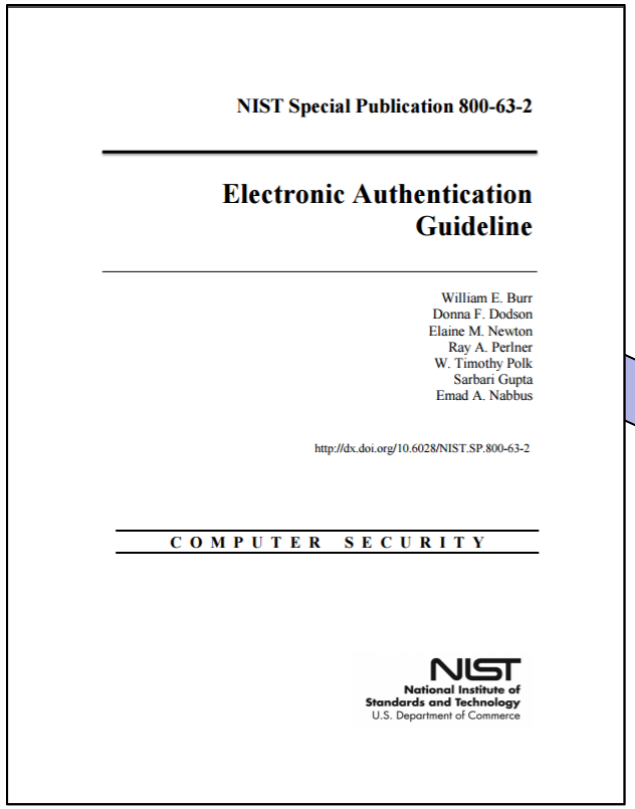
CertiPath

National Strategy for Trusted Identities in Cyberspace (NSTIC)

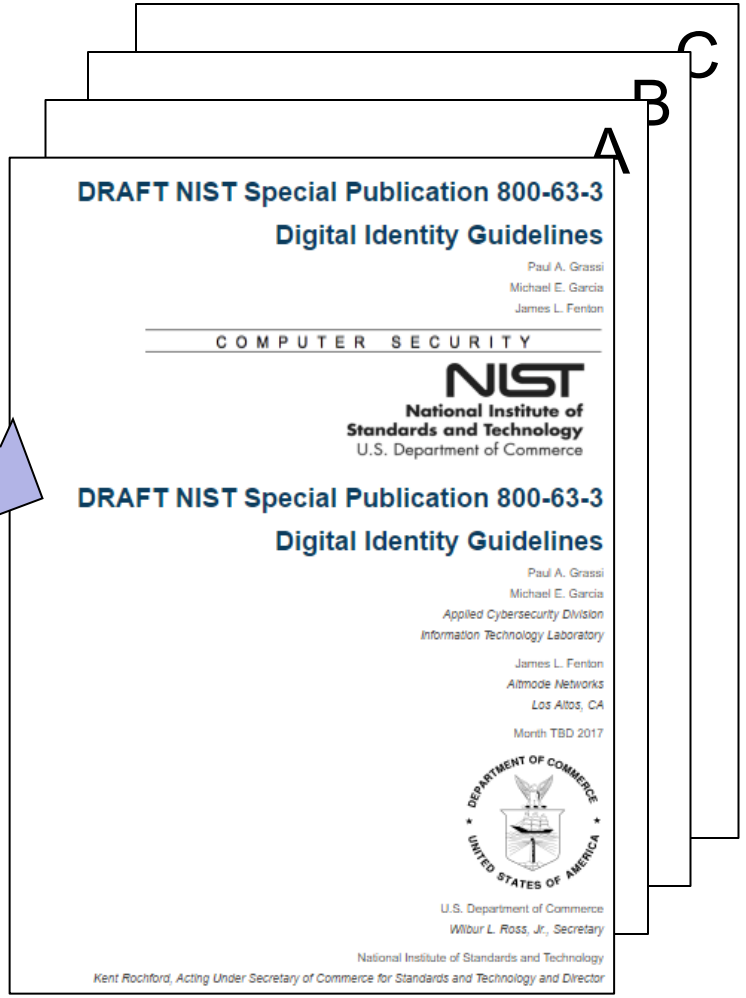
- A public/private partnership for improving the security and privacy of online transactions through trusted identities
- Establishing an identity *ecosystem* in the virtual world in which people can move about with confidence
- Removing the ambiguity & confusion, leading to better decision-making on the part of the consumer and the relying party
- NIST hosts the Trusted Identities Group for liaison with industry.
- Visit the web site at www.nist.gov/itl/tig to stay current on NIST activities
- Visit the Identity Ecosystem Steering Group (IDESG) at www.idesg.org to learn more about the industry initiative

CertiPath

SP 800-63-3 Digital Identity Guideline



becomes



CertiPath

SP 800-63-3 Digital Identity Guideline

Old

New

LOA

Level of Assurance

IAL

Identity Assurance Level

Robustness of the identity proofing process and the binding between an authenticator and a specific individual

AAL

Authentication Assurance Level

Confidence that a given claimant is the same as a subscriber that has previously authenticated

FAL

Federation Assurance Level

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

CertiPath

FICAM Playbooks

- Playbooks being created that focus on Part B: Implementation Guidance from the FICAM Roadmap https://fpki.idmanagement.gov/

Roadmap Chapter and Title	Playbook Title
Chapter 6: Implementation Planning	Program Management
Chapter 7: Streamline Collection and Sharing of Digital Identity Data	Streamline Identity Management
Chapter 8: Fully Leverage PIV Credentials	PIV Guides
Chapter 9: Access Control Convergence	Manage Access Control
Chapter 10: Modernize PACS	Physical Access Control Systems
Chapter 11: Modernize LACS	Logical Access Control Systems
Chapter 12: Implement Federation	Federation; FPKI Guides

FICAM Playbooks

Manage Access Control Playbook

Submit Issues Here
Playbook Home Page

Edit this page

Step 2 - Conduct a Policy Analysis

- Home
- Step 1 - Establish an Access Governance Structure
- Step 2 - Conduct a Policy Analysis
- Step 3 - Define Access Control Requirements
- Step 4 - Identify Protected Resources
- Step 5 - Conduct a Risk Assessment
- Access Management Framework
- Step 6 - Choose Your Access Control Model
- Step 7 - Establish the Data Management Life Cycle
- Step 8 - Establish the Privilege Management Life Cycle
- Step 9 - Establish the Policy Administration Life Cycle
- Step 10 - Manage the System Development Life Cycle
- Contribute

Conducting a policy analysis will help you better understand the existing access control expectations and limitations, the selection and implementation of access control measures, and supporting enablers to protect your agency's resources. Understanding your policies across the enterprise will help you update existing policies and draft new ones to support your agency's access control needs.

Checklist

☑ **Analyze existing policies.** Review your agency's access management policies to determine if they are aligned with the broader access control goals and objectives. This will help you determine if your agency should develop new policies to enforce appropriate access control requirements agency-wide.

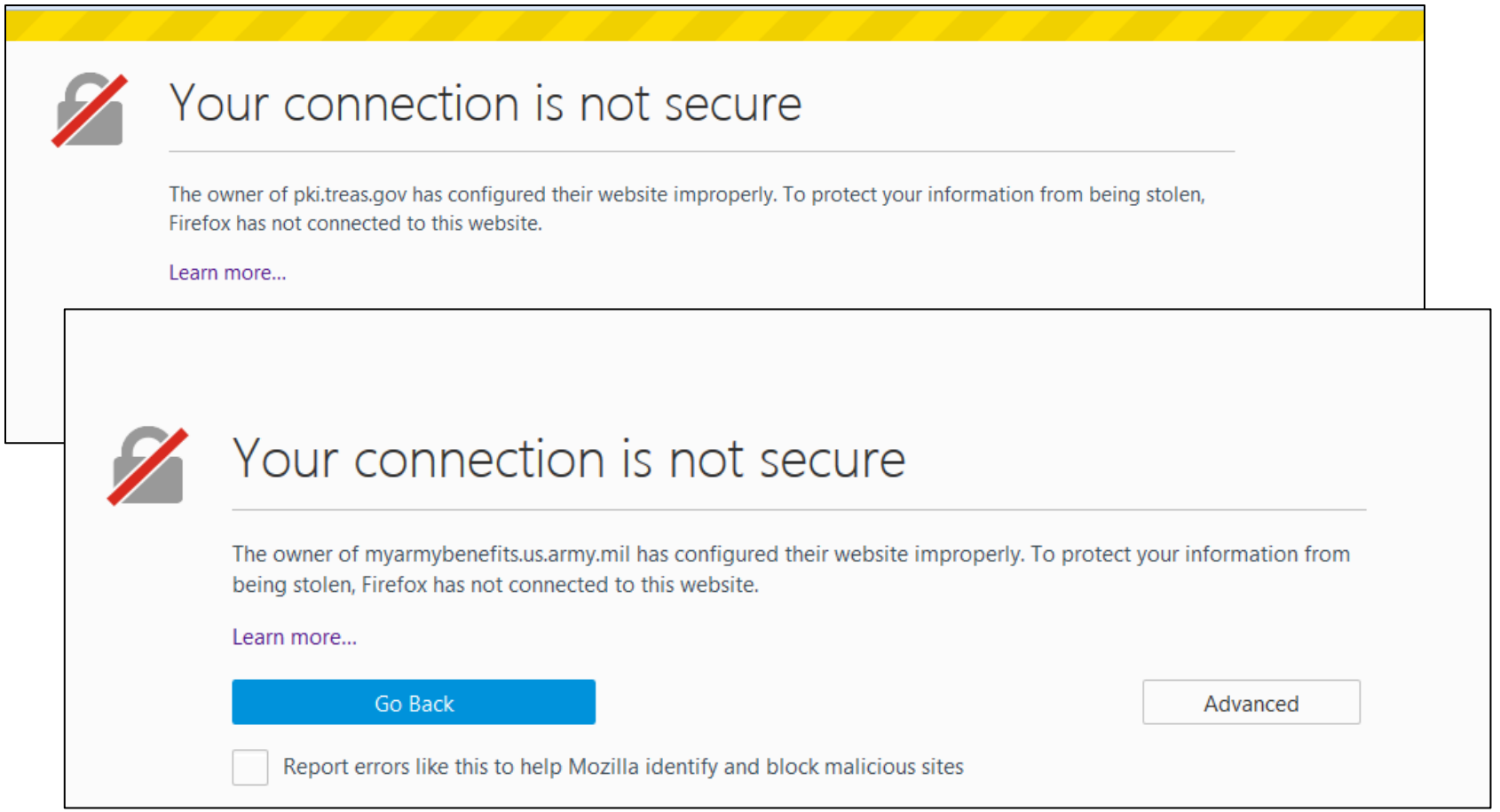
☑ **Establish baseline access control policies.** You should establish baseline access control policies that define minimum security requirements at the enterprise level. This helps you establish access control standards for protecting agency resources across the enterprise. Below are a few access control management policy examples.

Potential Access Policies	Description
Issue Policy Memorandum: Continued Implementation of HSPD-12	Enforcing use of the PIV card for physical and logical access and acceptance of PIV credentials issued by other federal agencies.
Issue Policy/Guidance Addressing Common Physical Scenarios and Common Logical Access Scenarios	Formal agency-level decisions for handling common physical and logical access scenarios such as a lost/forgotten PIV card or forgotten personal identification number (PIN).
Issue Policy/Guidance Addressing Standardization of Local Facility Access Cards	Policy or procedural guidance for establishing a standard local facility access card and providing guidance around when and how they are issued.
Issue Policy/Guidance Addressing Visitor Management	Procedural guidance for establishing what types of credentials are considered acceptable for granting physical access to visitors, including individuals who are not PIV card holders (e.g., escort procedures).

- Web-based
- Navigable
- Usable
- Plain Language

CertiPath

FPKI TLS Root Initiative



CertiPath

TLS CA Scope

In Scope

Certificates for web services on the public Internet

DotGov and DotMil

Govt option for Certificate Transparency logs, commercial logging, and support

NOT In Scope

Code signing certificates

Other *domains*
**.edu*
**.com*
**.org*

Person certificates (PIV) including authentication, digital signature and encryption

CertiPath

Following Industry Lead

Technology

- Certificate Transparency (CT) for public devices
- Increasingly shorter lifetimes for certificates

Public Trust requirements are defined by the Browsers and Trust Stores community:
US Government is only one participant in a broad ecosystem for Internet Security

Plans	Certificate Transparency
When	April 2018+
How	Buy certificates that include CT logging

Plans	Shorter lifetimes
When	March 2018+
How	Two year *or* less lifetimes

CertiPath

Objectives

Update Federal PKI

- Public trust of government issued certificates for government websites
- More agile approach
- Respond to Internet Security requirements faster
- Provide our community the services they expect and deserve

1. Create a policy consistent with standards specific to Public Trust and web services

2. Create a government-wide shared solution to enable automation, scaling and management of public trust website certificates

CertiPath

What's Next?

- Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017)
  - Emphasis on shared IT services & consolidated network architecture

Thank you

Judith Spencer
CertiPath PMA Chair
judith.spencer@certipath.com

CertiPath