FPKIPA
Federal Public Key Infrastructure Policy Authority

NIST
National Institute of
Standards and Technology

Computer Security
Program Managers Forum

FPKI Profile of NIST SP 800-53 Overview and Approach

6 December 2011
Matt King

Agenda

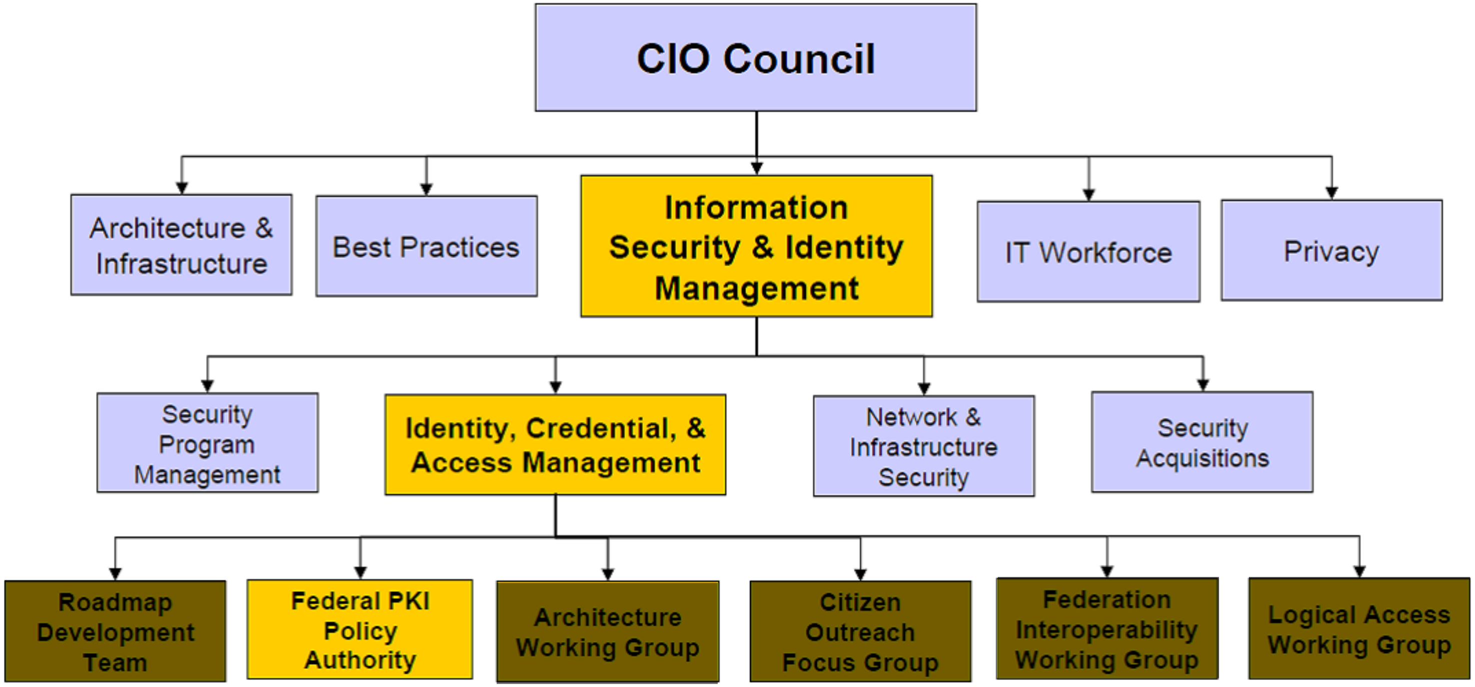
- FPKI Background
- FPKI Profile Concept
- Approach
- Samples
- Questions

FPKI Background and History

- First Federal Bridge Certificate Authority (FBCA) Certificate Policy approved in 2000
  - Serves as a interoperability mechanism for ensuring trust across disparate PKI domains
  - Cross certification asserts that a PKI operates in accordance with FBCA Policy
- FPKI Architecture expanded to include the Federal PKI Common Policy Framework CA (FCPCA), and E-Governance Trust Services (EGTS)
  - The FCPCA is the Trust Anchor for the U.S. Federal Government
  - EGTS facilitates the use of federated identity
    - Throughout the Federal Government; and
    - Between the Federal Government and external partners

FPKI Lines of Authority

- The FPKI Policy Authority (FPKIPA) sets policy governing operation of the FBCA, the FCPCA, and the EGTS
  - Operates under the authority of the Federal CIO Council


CIO Council

Architecture & Infrastructure

Best Practices

Information Security & Identity Management

IT Workforce

Privacy

Security Program Management

Identity, Credential, & Access Management

Network & Infrastructure Security

Security Acquisitions

Roadmap Development Team

Federal PKI Policy Authority

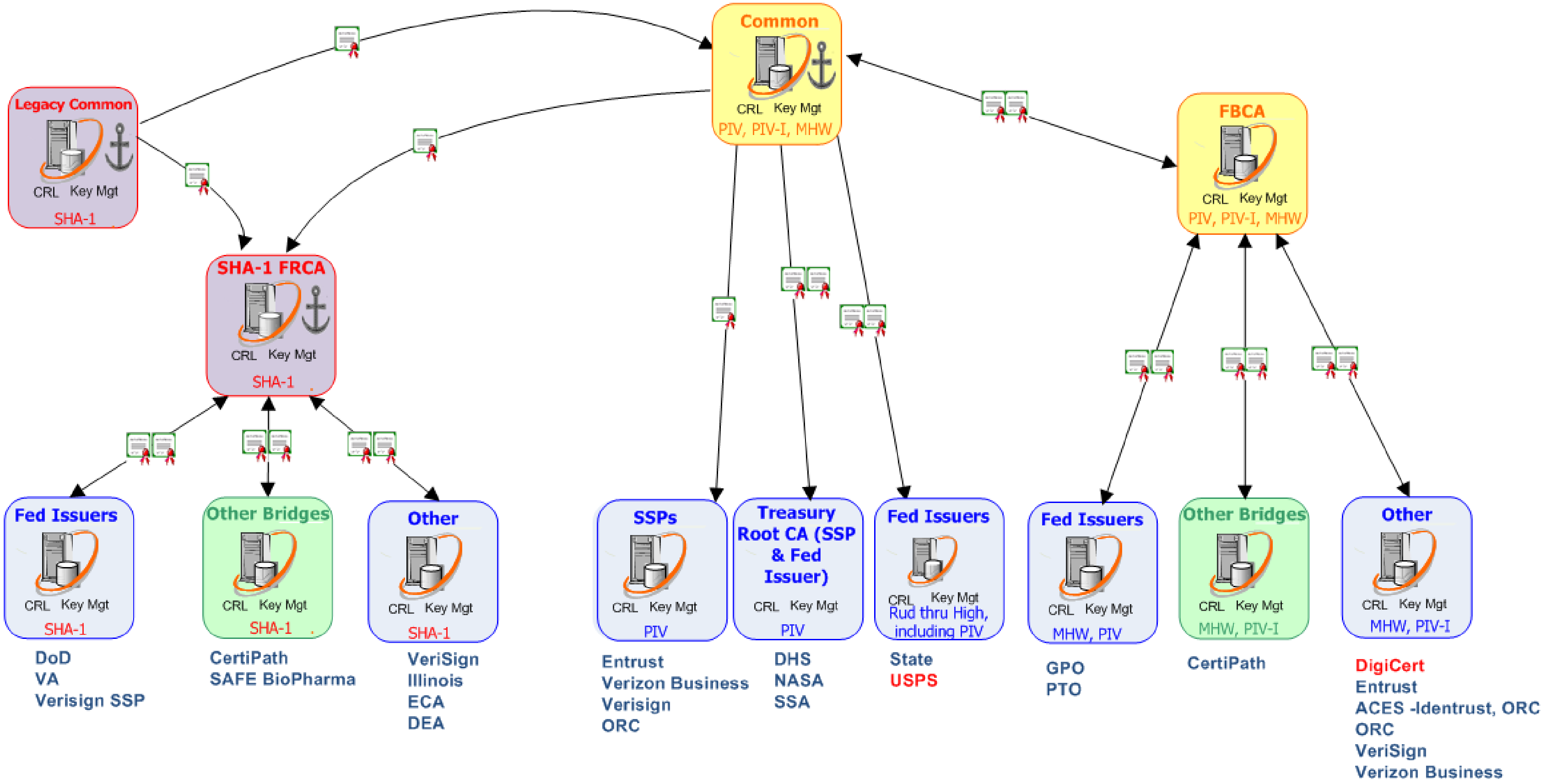
Architecture Working Group

Citizen Outreach Focus Group

Federation Interoperability Working Group

Logical Access Working Group

FPKI Architecture Overview



Common
PIV, PIV-I, MHW

Legacy Common
SHA-1

FBCA
PIV, PIV-I, MHW

SHA-1 FRCA
SHA-1

Fed Issuers
SHA-1
DoD
VA
Verisign SSP

Other Bridges
SHA-1
CertiPath
SAFE BioPharma

Other
SHA-1
VeriSign
Illinois
ECA
DEA

SSPs
PIV
Entrust
Verizon Business
Verisign
ORC

Treasury Root CA (SSP & Fed Issuer)
PIV
DHS
NASA
SSA

Fed Issuers
Rud thru High, including PIV
State
USPS

Fed Issuers
MHW, PIV
GPO
PTO

Other Bridges
MHW, PIV-I
CertiPath

Other
MHW, PIV-I
DigiCert
Entrust
ACES -Identrust, ORC
ORC
VeriSign
Verizon Business

FBCA and the Common Policy CA (i.e., FCPCA) are cross-certified, which allows path validation across the FBCA to the Federal Trust Anchor

Agenda

- ✓ FPKI Background
- FPKI Profile Concept
- Approach
- Samples
- Questions

FPKI Profile Concept: Overview of NIST SP 800-53

- NIST SP 800-53 = Requirements
  - Lists specific requirements for evaluation by assessors
  - Includes Low, Moderate and High Baselines (FIPS-199)
    - The FPKI Profile is really a profile of the High Baseline
- NIST SP 800-53A = Guidance to assessors
  - Restates requirements with assessment guidance
- To summarize:
  - SP 800-53 lists specific requirements for WHAT is evaluated by assessors
  - SP 800-53A describes HOW those requirements will be evaluated

FPKI Profile Concept: Why Create a FPKI Profile?

- PKIs are *Infrastructures*
  - PKIs support other applications, systems, and networks and provide:
    - Identity authentication
    - Technical non-repudiation
    - Data integrity and
    - Confidentiality
  - Therefore, PKIs require higher levels of security, access control, and operational rigor than the data and systems they protect
  - In addition, certain provisions and techniques specified in SP 800-53 were incompatible with PKI system and the FPKI certificate policy requirements

FPKI Profile Concept: Why Create a FPKI Profile?

- Applying the FPKI Profile will result in:
  - Standard application of security controls in PKIs across Government
    - Specifies security controls unique to and critical for PKI operation
    - Standardizes the way PKIs Security Assessments are performed
  - Cost savings
    - The FPKI Profile reduces assessor time and staff required to determine what requirements to evaluate and how
  - Enhanced the Trust across the Government
    - Builds upon the assurance provided by Policy Mapping

Agenda

- ✓ FPKI Background
- ✓ FPKI Profile Concept
- Approach
- Samples
- Questions

Approach – Development

- Established a Special Multi-Agency WG comprised of FPKI Member Agencies
  - Including State, DoD, Treasury, DHS and others
- Started with the High Baseline of NIST 800-53
  - PKI's strength relies on its Trust Model – trust that spans all agencies
  - The Trust Model relies on limited access, rigorous specified procedures & configurations, external compliance audits, as well as IT security
- Populated a document to develop content
  - Included all High Impact Baseline controls and enhancement
  - For each control, we asked: "Anything special for PKI?"
  - Tailored the controls for PKI:
    - Added, modified or removed control text / enhancements
  - Developed associated assessment guidance

Approach – Buy In and Enforcement

- Developed profiles of 800-53 and 800-53A
- Profiles were reviewed by the FPKI CPWG and NIST
- Requested comments and agreement with the profile from the Federal CIO community including the ICAMSC and ISIMC
- Worked with OMB to establish mechanism for PKI Systems across the Government to report compliance with the FPKI Security Control Profiles
  - Inserted a requirement into the 2012 FISMA Annual Reporting Metrics requiring Agency PKIs to comply with the Profile

Agenda

- ✓ FPKI Background
- ✓ FPKI Profile Concept
- ✓ Approach
- ▪ Samples
- ▪ Questions

Sample: 800-53 Requirement Baselines

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5

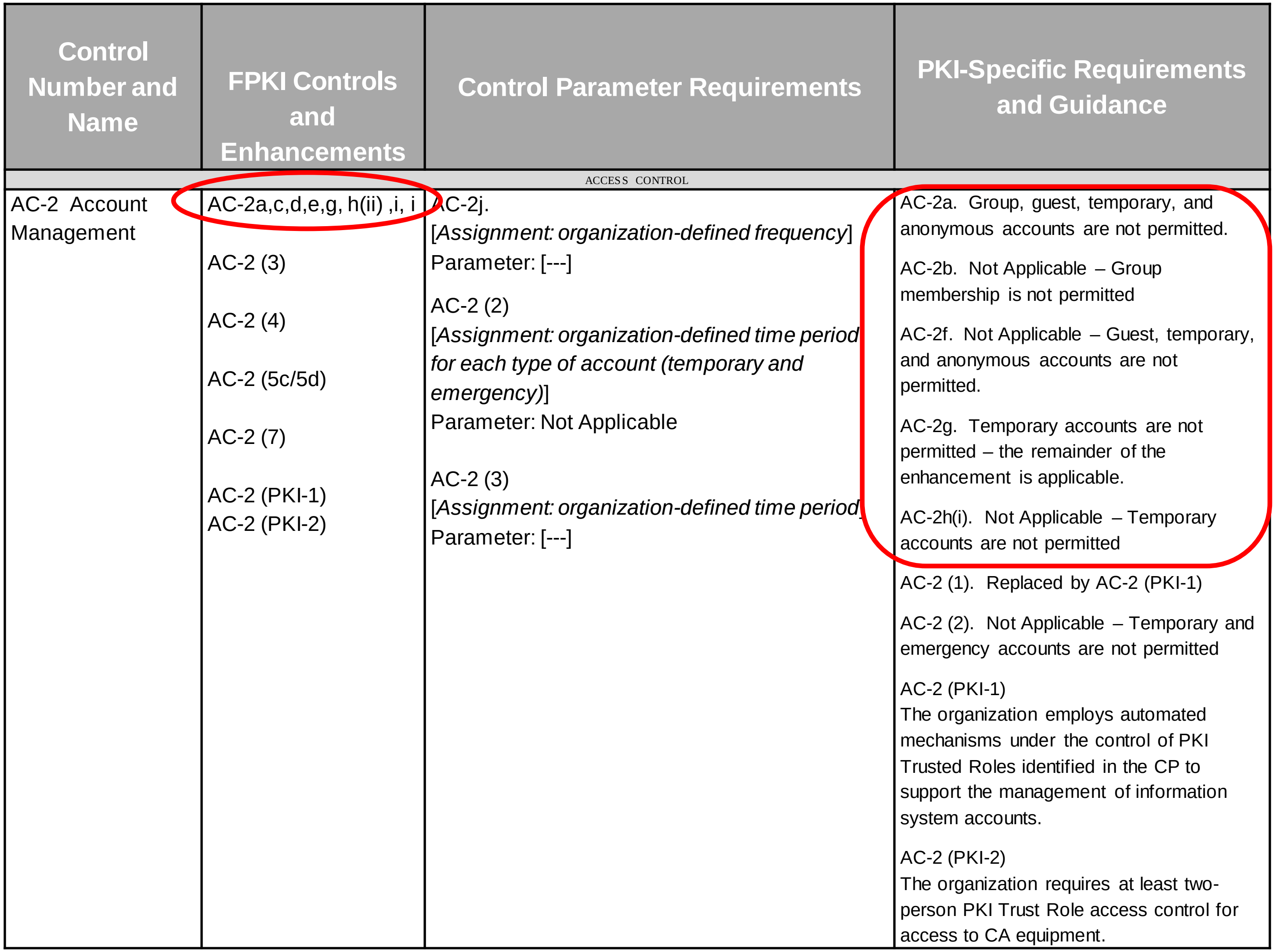
Sample: 800-53 AC-2: Control Text

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:

a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
b. ~~Establishing conditions for group membership;~~
c. Identifying authorized users of the information system and specifying access privileges;
d. Requiring appropriate approvals for requests to establish accounts;
e. Establishing, activating, modifying, disabling, and removing accounts;
f. ~~Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;~~
g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
h. Deactivating: ~~(i) temporary accounts that are no longer required;~~ and (ii) accounts of terminated or transferred users;
i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
j. Reviewing accounts [*Assignment: organization-defined frequency*].

Sample: FPKI Profile of 800-53



Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
ACCESS CONTROL			
AC-2 Account Management	AC-2a,c,d,e,g, h(ii) ,i, i AC-2 (3) AC-2 (4) AC-2 (5c/5d) AC-2 (7) AC-2 (PKI-1) AC-2 (PKI-2)	AC-2j. [*Assignment: organization-defined frequency*] Parameter: [---] AC-2 (2) [*Assignment: organization-defined time period for each type of account (temporary and emergency)*] Parameter: Not Applicable AC-2 (3) [*Assignment: organization-defined time period*] Parameter: [---]	AC-2a. Group, guest, temporary, and anonymous accounts are not permitted. AC-2b. Not Applicable – Group membership is not permitted AC-2f. Not Applicable – Guest, temporary, and anonymous accounts are not permitted. AC-2g. Temporary accounts are not permitted – the remainder of the enhancement is applicable. AC-2h(i). Not Applicable – Temporary accounts are not permitted AC-2 (1). Replaced by AC-2 (PKI-1) AC-2 (2). Not Applicable – Temporary and emergency accounts are not permitted AC-2 (PKI-1) The organization employs automated mechanisms under the control of PKI Trusted Roles identified in the CP to support the management of information system accounts. AC-2 (PKI-2) The organization requires at least two-person PKI Trust Role access control for access to CA equipment.

Sample: 800-53 Requirement Baselines

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5

Sample: 800-53 AC-2: Control Enhancements

Control Enhancements:

1. **The organization employs automated mechanisms to support the management of information system accounts.**
2. **The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].**
3. **The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].**
4. **The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.**
5. **The organization:**
    a. **Requires that users log out when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*];**
    b. **Determines normal time-of-day and duration usage for information system accounts;**
    c. **Monitors for atypical usage of information system accounts; and**
    d. **Reports atypical usage to designated organizational officials.**
6. **The information system dynamically manages user privileges and associated access authorizations.**

    Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain relatively constant over time, user privileges may change more frequently based on the ongoing mission/business requirements and operational needs of the organization.
7. **The organization:**
    a. **Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and**
    b. **Tracks and monitors privileged role assignments.**

    Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.

Sample: FPKI Profile of 800-53

Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
ACCESS CONTROL			
AC-2 Account Management	AC-2a,c,d,e,g, h(ii) ,i, i AC-2 (3) AC-2 (4) AC-2 (5c/5d) AC-2 (7) AC-2 (PKI-1) AC-2 (PKI-2)	AC-2j. [*Assignment: organization-defined frequency*] Parameter: [---] AC-2 (2) [*Assignment: organization-defined time period for each type of account (temporary and emergency)*] Parameter: Not Applicable AC-2 (3) [*Assignment: organization-defined time period*] Parameter: [---]	AC-2a. Group, guest, temporary, and anonymous accounts are not permitted. AC-2b. Not Applicable – Group membership is not permitted AC-2f. Not Applicable – Guest, temporary, and anonymous accounts are not permitted. AC-2g. Temporary accounts are not permitted – the remainder of the enhancement is applicable. AC-2h(i). Not Applicable – Temporary accounts are not permitted AC-2 (1). Replaced by AC-2 (PKI-1) AC-2 (2). Not Applicable – Temporary and emergency accounts are not permitted AC-2 (PKI-1) The organization employs automated mechanisms under the control of PKI Trusted Roles identified in the CP to support the management of information system accounts. AC-2 (PKI-2) The organization requires at least two-person PKI Trust Role access control for access to CA equipment.

Sample: 800-53 AC-2: Control Enhancements

Control Enhancements:

1. **The organization employs automated mechanisms to support the management of information system accounts.**
2. **The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].**
3. **The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].**
4. **The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.**
5. **The organization:**
   - a. **Requires that users log out when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*];**
   - b. **Determines normal time-of-day and duration usage for information system accounts;**
   - c. **Monitors for atypical usage of information system accounts; and**
   - d. **Reports atypical usage to designated organizational officials.**
6. **The information system dynamically manages user privileges and associated access authorizations.**

   Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain relatively constant over time, user privileges may change more frequently based on the ongoing mission/business requirements and operational needs of the organization.
7. **The organization:**
   - a. **Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and**
   - b. **Tracks and monitors privileged role assignments.**

   Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.

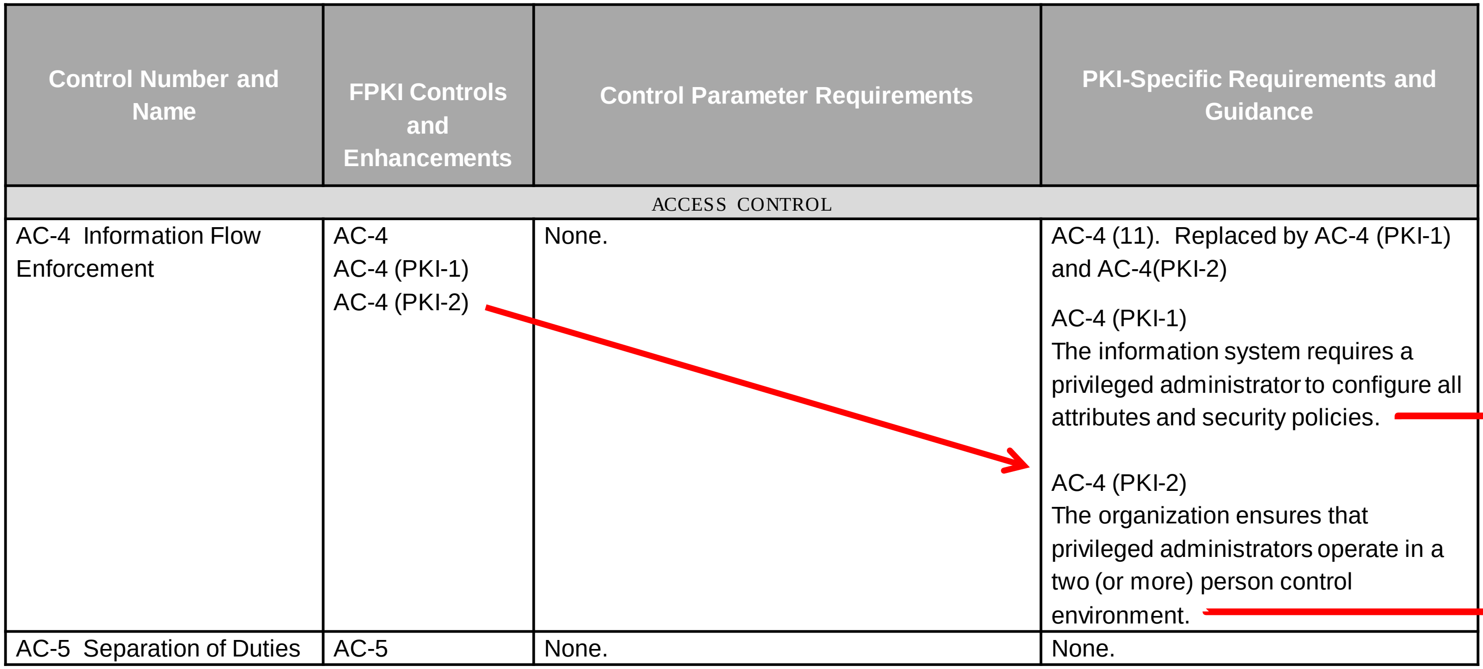
AC-2 (PKI-1) The organization employs automated mechanisms under the control of PKI Trusted Roles identified in the CP to support the management of information system accounts.

AC-2 (PKI-2) The organization requires at least two-person PKI Trust Role access control for access to CA equipment.

Sample: FPKI Profile of 800-53A (Assessment Guidance)

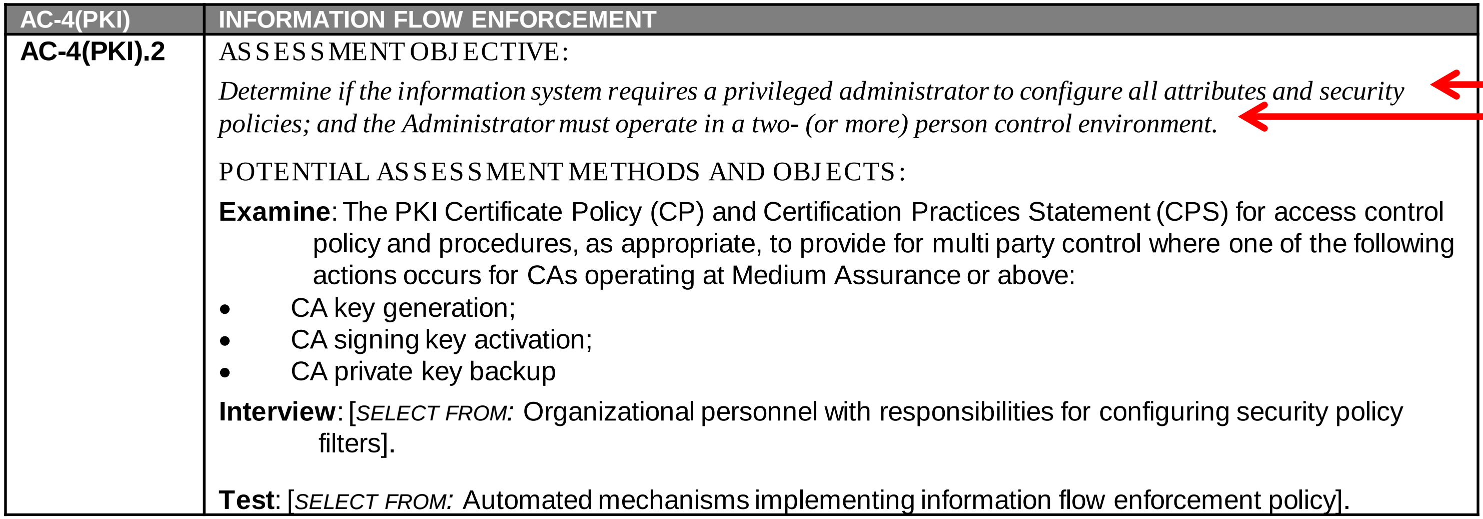
AC-2	ACCOUNT MANAGEMENT
AC-2.1	ASSESSMENT OBJECTIVE: *Determine if:* *(i) the organization manages information system accounts, including;* - *group, guest, temporary, anonymous accounts are not permitted;* - *identifying authorized users of the information system and specifying access privileges;* - *requiring appropriate approvals for requests to establish accounts;* - *establishing, activating, modifying, disabling, and removing accounts;* - *notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;* - *deactivating: i) temporary accounts that are no longer required; and ii) accounts of terminated or transferred users; and* - *granting access to the system based on:* - *a valid access authorization;* - *intended system usage; and* - *other attributes as required by the organization or associated missions/business functions; and* *(i) the organization defines the frequency of information system account reviews; and* *(ii) the organization reviews information system accounts in accordance with organization-defined frequency.* POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures as specified for AC-2 with the following modification and enhancements: • Group, guest, temporary, anonymous accounts are not permitted • Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes • Deactivating accounts of terminated or transferred users • Monitors for atypical usage of information system accounts; and reports atypical usage to designated organizational officials • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and tracks and monitors privileged role assignments **Interview**: [*SELECT FROM:* Organizational personnel with account management responsibilities].

Sample: FPKI Profile of 800-53



Control Number and Name	FPKI Controls and Enhancements	Control Parameter Requirements	PKI-Specific Requirements and Guidance
ACCESS CONTROL			
AC-4 Information Flow Enforcement	AC-4 AC-4 (PKI-1) AC-4 (PKI-2)	None.	AC-4 (11). Replaced by AC-4 (PKI-1) and AC-4(PKI-2) AC-4 (PKI-1) The information system requires a privileged administrator to configure all attributes and security policies. AC-4 (PKI-2) The organization ensures that privileged administrators operate in a two (or more) person control environment.
AC-5 Separation of Duties	AC-5	None.	None.

Sample: FPKI Profile of 800-53A (Assessment Guidance)



AC-4(PKI)	INFORMATION FLOW ENFORCEMENT
AC-4(PKI).2	ASSESSMENT OBJECTIVE: *Determine if the information system requires a privileged administrator to configure all attributes and security policies; and the Administrator must operate in a two- (or more) person control environment.* POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: The PKI Certificate Policy (CP) and Certification Practices Statement (CPS) for access control policy and procedures, as appropriate, to provide for multi party control where one of the following actions occurs for CAs operating at Medium Assurance or above: • CA key generation; • CA signing key activation; • CA private key backup **Interview**: [*SELECT FROM:* Organizational personnel with responsibilities for configuring security policy filters]. **Test**: [*SELECT FROM:* Automated mechanisms implementing information flow enforcement policy].

Agenda

- ✓ FPKI Background
- ✓ FPKI Profile Concept
- ✓ Approach
- ✓ Samples
- ▪ Questions

Questions?

Matt King
Matthew.King@pgs.protiviti.com

410-271-5624

protiviti®
Risk & Business Consulting.
Internal Audit.
GOVERNMENT SERVICES