Cryptographic Key Management Workshop

March 4-5, 2014

Session 2: Basic Concepts and Security Policies
(SP 800-152, Sections 1, 4 & 5)

Elaine Barker and Dennis Branstad

FCKMS vs. CKMS

CKMS:

- Created by a designer/implementer
- **Shall** satisfy Framework requirements.
- Implementation **shall** support all capabilities of the design (PR:2.7).
- **Could** include switches to turn capabilities off or on for customizing to become an FCKMS.

FCKMS vs. CKMS (contd.)

CKMS

General capabilities:

- Encrypt/decrypt
- Generate/verify digital signatures

Optional capabilities:

- Option A (AES-128)
- Option B (3TDEA)
- Option C (SHA-1)
- Option D (SHA-256)
- Option E (RSA)
- Option F (ECDSA)

FCKMS vs. CKMS (contd.)

FCKMS:

- A configured CKMS for use by the Federal government.
- Uses a CKMS that is compliant with the Framework and capable of supporting the Profile.
- Configured by the service provider for the service users.
- Capabilities are selected from those provided in the chosen CKMS product.

FCKMS vs. CKMS (contd.)

FCKMS X

General capabilities:

- Encrypt/decrypt
- Generate/verify digital signatures

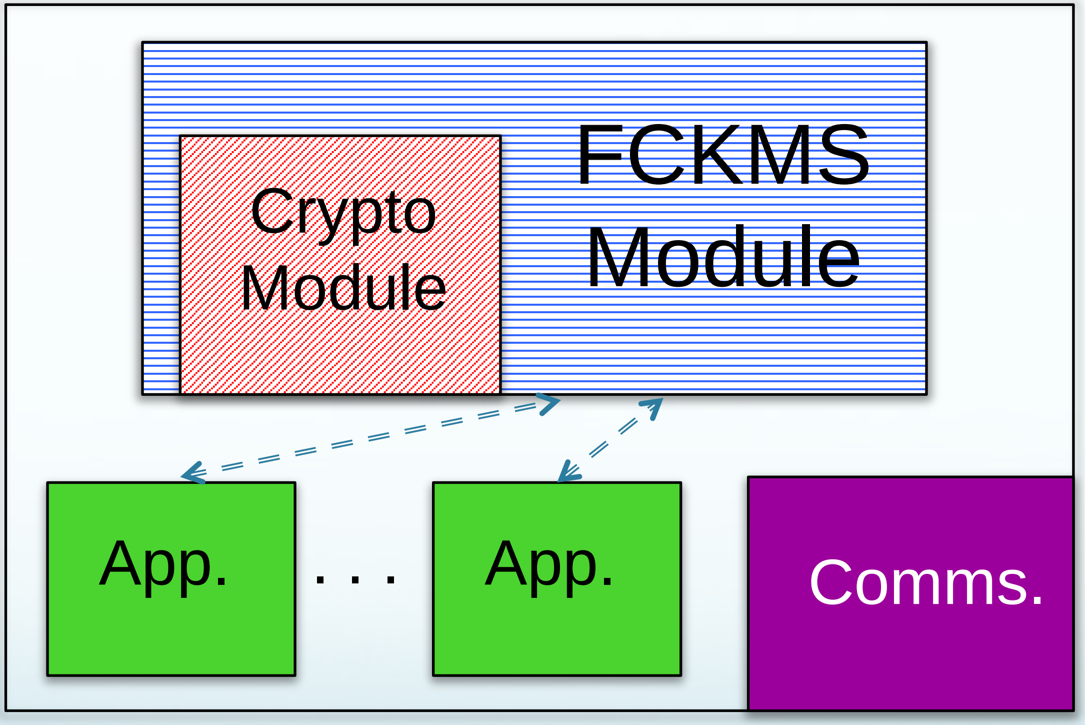
Optional capabilities:

- Option A (AES-128)
- Option D (SHA-256)
- Option E (RSA)
- Option F (ECDSA)

CKMS/FCKMS Modules

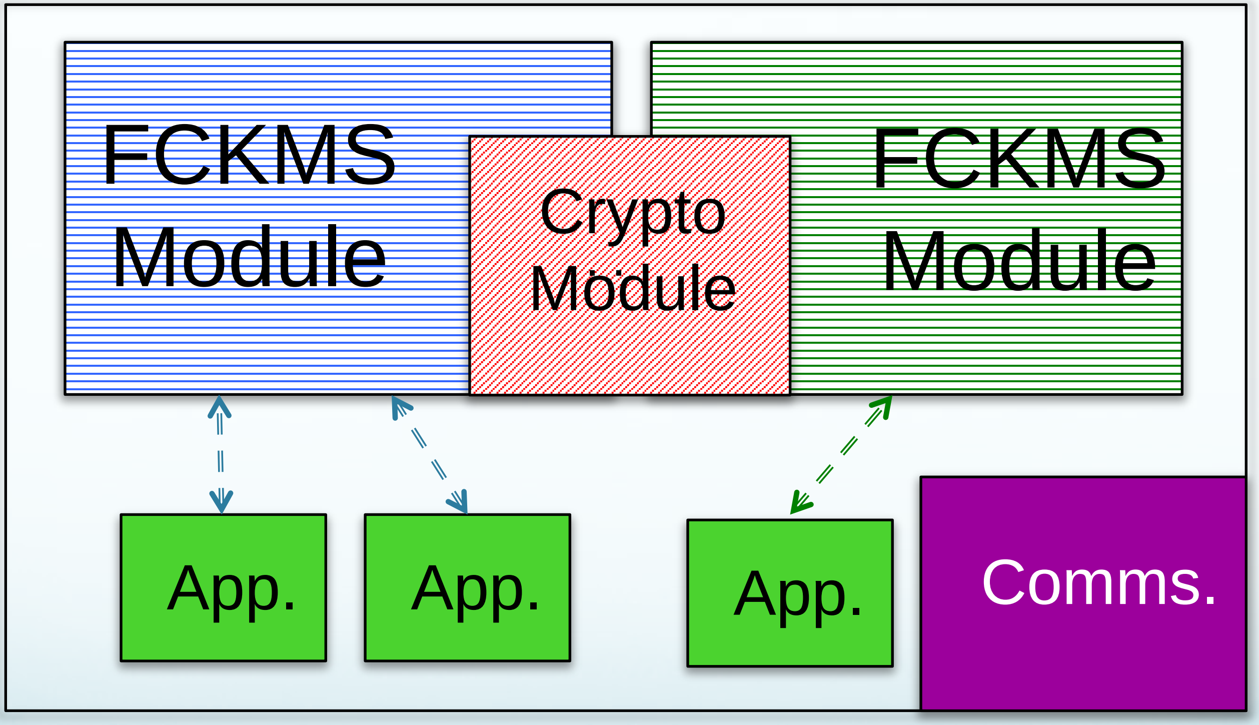
- Each module contains some or all of the CKMS/FCKMS functionality.
- Accesses or incorporates a cryptographic module.
- Is or resides within some device.
- Software, firmware, hardware or a combination.

CKMS/FCKMS Entity Example



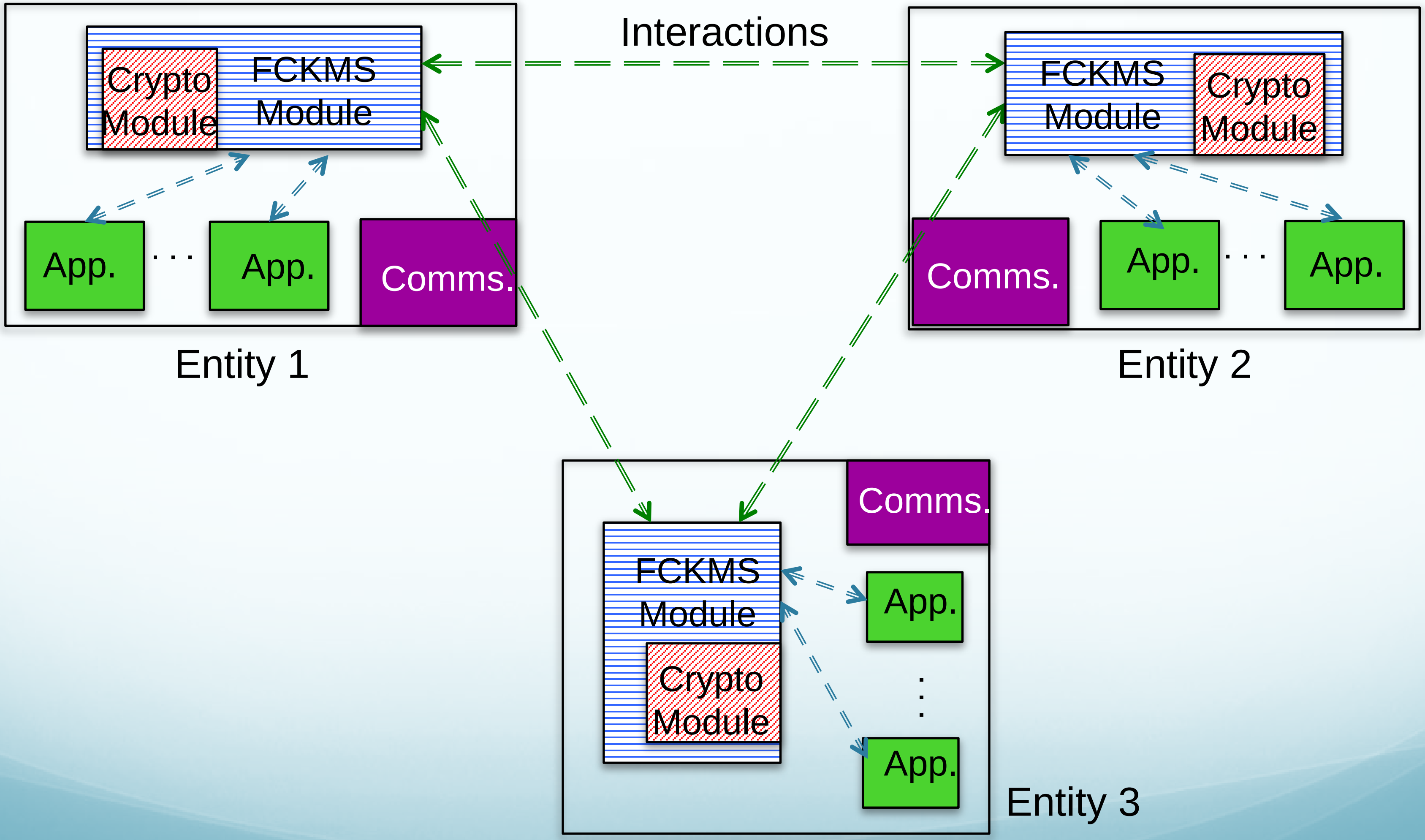
Entity: Server/Laptop/Smart phone, etc.

Another CKMS/FCKMS Entity Example

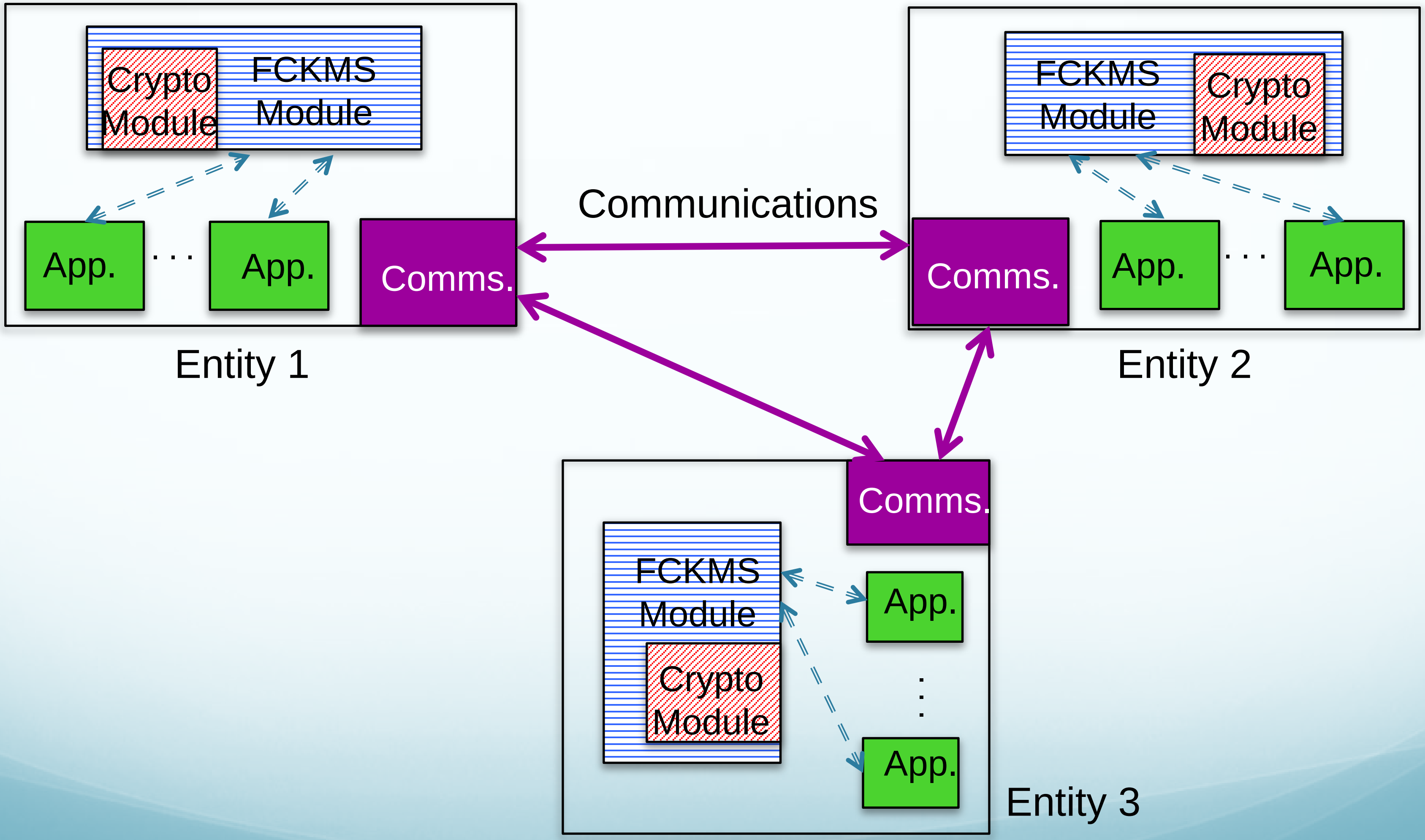


Entity: Server/Laptop/Smart phone, etc.

FCKMS (Network)



FCKMS "Network"



Security Policies (Section 4)

Policy	CKMS Designer/implementer	Service Provider	Service User
Information Mgmt. Policy		?	D
Information Security Policy		?	D
CKMS Security Policy	D		
FCKMS Security Policy		D	R
FCKMS Module Security Policy ?		D	D/R
Cryptographic Module Security Policy		R	R
Domain Security Policy		?	?

D = Develop the policy R = Review the policy

Information Management Policy (Section 4.1)

- Governs the collection, processing, and use of an organization’s information, and specifies what information is to be collected or created, and how it is to be managed.
- Established using industry standards of good practices, legal requirements regarding the organization’s information, and organizational goals to be achieved using the information that the organization will be collecting and creating.
- Required by PR: 4.1 for an FCKMS service-using organization.
- Is a PR or PA appropriate for the FCKMS service-providing organization as well?

Information Security Policy (Section 4.2)

- Supports and enforces portions of the organization’s Information Management Policy – provides more details about what information is to be protected from anticipated threats and how that protection is to be attained.
- Required by PR: 4.2 for an FCKMS service-using organization.
- Is a PR or PA appropriate for the FCKMS service-providing organization as well?

Computer Security Policy (Section 4.4.2)

- Specifies how the information is to be protected while being processed and stored in a computer system.
- Should be based on and support an Information Security Policy.
- Recommended for an FCKMS service-using organization in PA:4.6). Should this be a PR?
- Should this policy even be included in the Profile?

CKMS Security Policy (Section 4.3)

- Specifies the methods used in the CKMS design to create, use and protect the cryptographic keys and metadata and any restrictions associated with their use.
- Should cover the entire key lifecycle, including when they are operational, stored, and transported.
- Includes an identification of all cryptographic mechanisms and cryptographic protocols that can be used by the CKMS.
- Required for the CKMS designer in SP 800-130 in FR: 4.1 (other FRs refer to the content).

FCKMS Security Policy
(Section 4.3)

- Intended to support the Information Security Policies of all the FCKMS service-using organizations.
- Specifies the rules for managing the cryptographic keys and metadata used to protect the user's information.
- May be identical to the CKMS Security Policy or may be a configured subset of that policy.
- Created by the FCKMS service provider and service user.
- Recommended for an FCKMS by PA: 4.1, including its content. Should the policy be required (i.e., changed to a PR)?
- Is this really a Domain Security Policy?

FCKMS Module Security Policy (Section 4.4.3)

- Supports the responsibilities to be assumed by the FCKMS Module (e.g., server, master, slave, peer).
- May not be the same as other FCKMS modules with which it interacts.
- May support multiple FCKMSs.
- May need to separate keys and metadata because of supporting multiple FCKMSs.
- Required in PR: 4.6.Should this be a PA?
- Should there even be such a policy? Could talk about capabilities instead.

Cryptographic Module Security Policy (Section 4.4.4)

- States the rules that the cryptographic module will follow when performing cryptographic functions (e.g., key generation and signature verification).
- Specifies the mechanisms to be used to maintain the security of the module and to protect sensitive data.
- Includes specifications for controlling access to the keys and metadata, the physical security provided to protect the module's storage and processing capabilities, and the mitigation of other attacks specified in the policy.

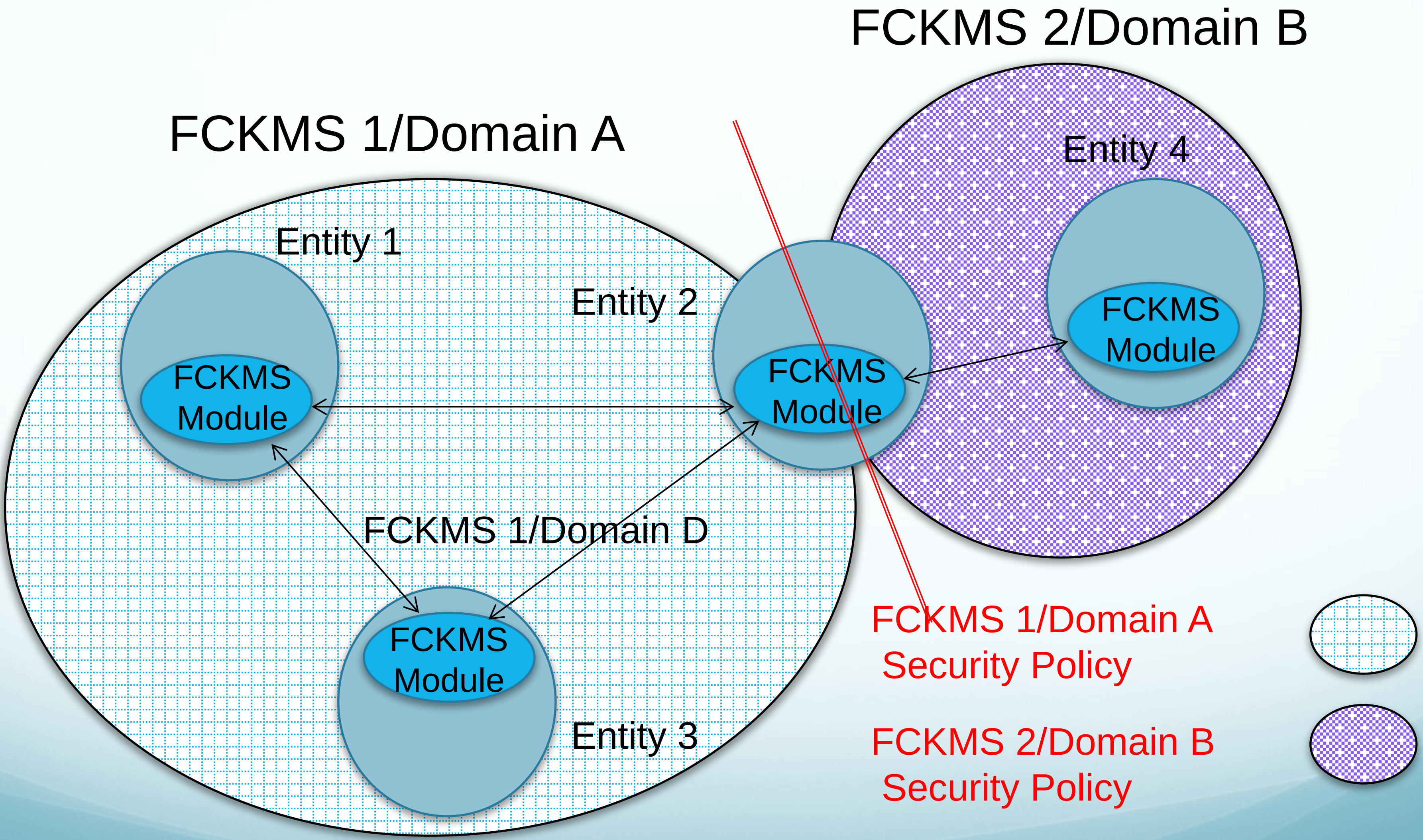
Cryptographic Module Security Policy (Section 4.4.4)

- Required indirectly by PR:2.9, which requires FIPS 140-validated modules.
    - Note: FIPS 140 requires this policy.
- May need to separate keys and metadata between applications/FCKMSs (required by PR:4.7 in certain situations).

FCKMS and Domains

- FCKMS: the CKMS that is used by the Federal government, possibly after configuring to meet the needs of an FCKMS service-using organization. Note that there is (currently) an FCKMS Security Policy.
- Domain: A collection of entities, including their FCKMSs, that support the same security policy (a Domain Security Policy).
- Are they the same thing?

Two FCKMSs/Domains



FCKMS 2/Domain B

FCKMS 1/Domain A

Entity 4

Entity 1

Entity 2

FCKMS Module

FCKMS Module

FCKMS Module

FCKMS 1/Domain D

FCKMS Module

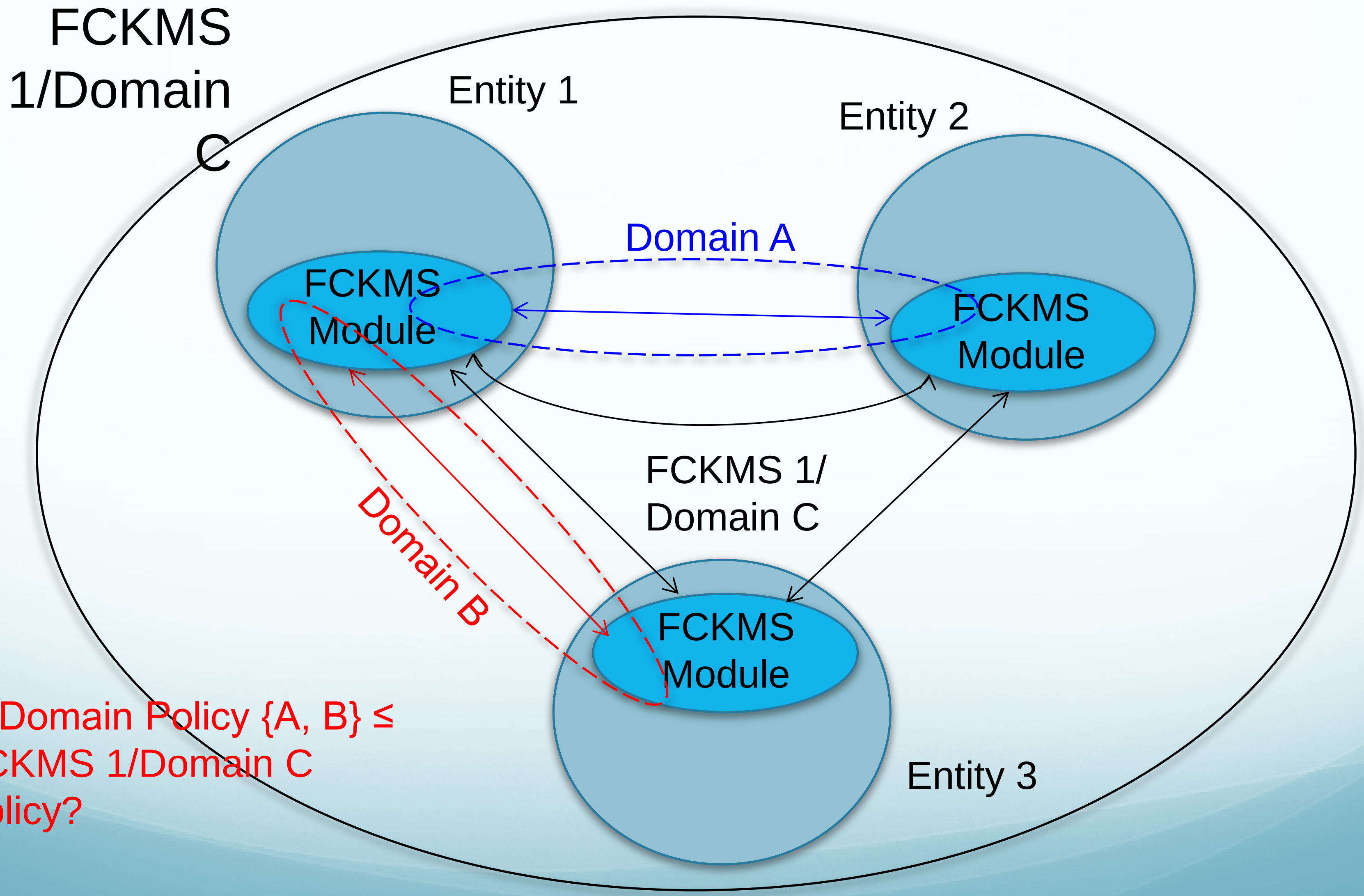
Entity 3

FCKMS 1/Domain A Security Policy ▦

FCKMS 2/Domain B Security Policy ▩

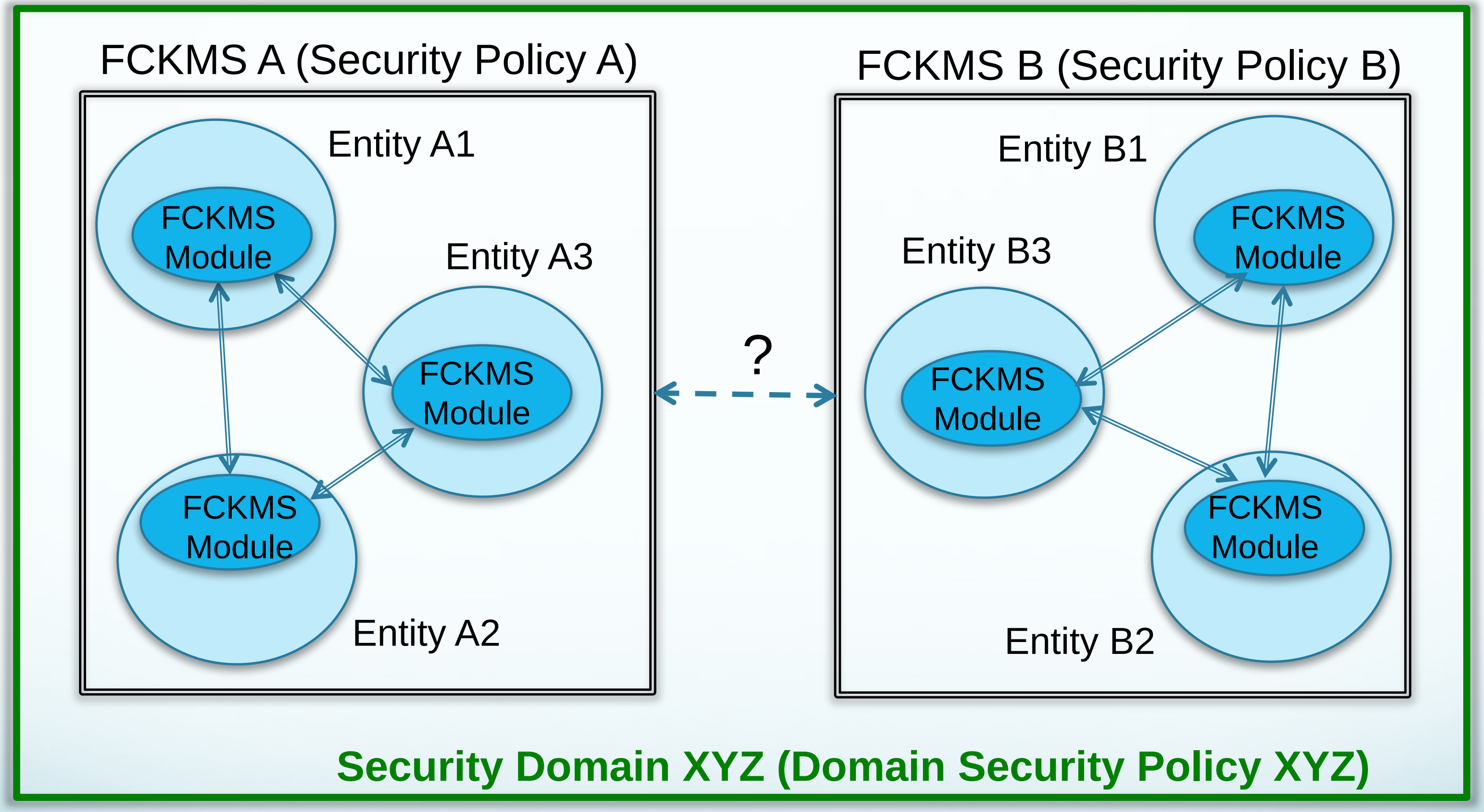
Entity 2 has both policies

FCKMS and “Internal” Domains



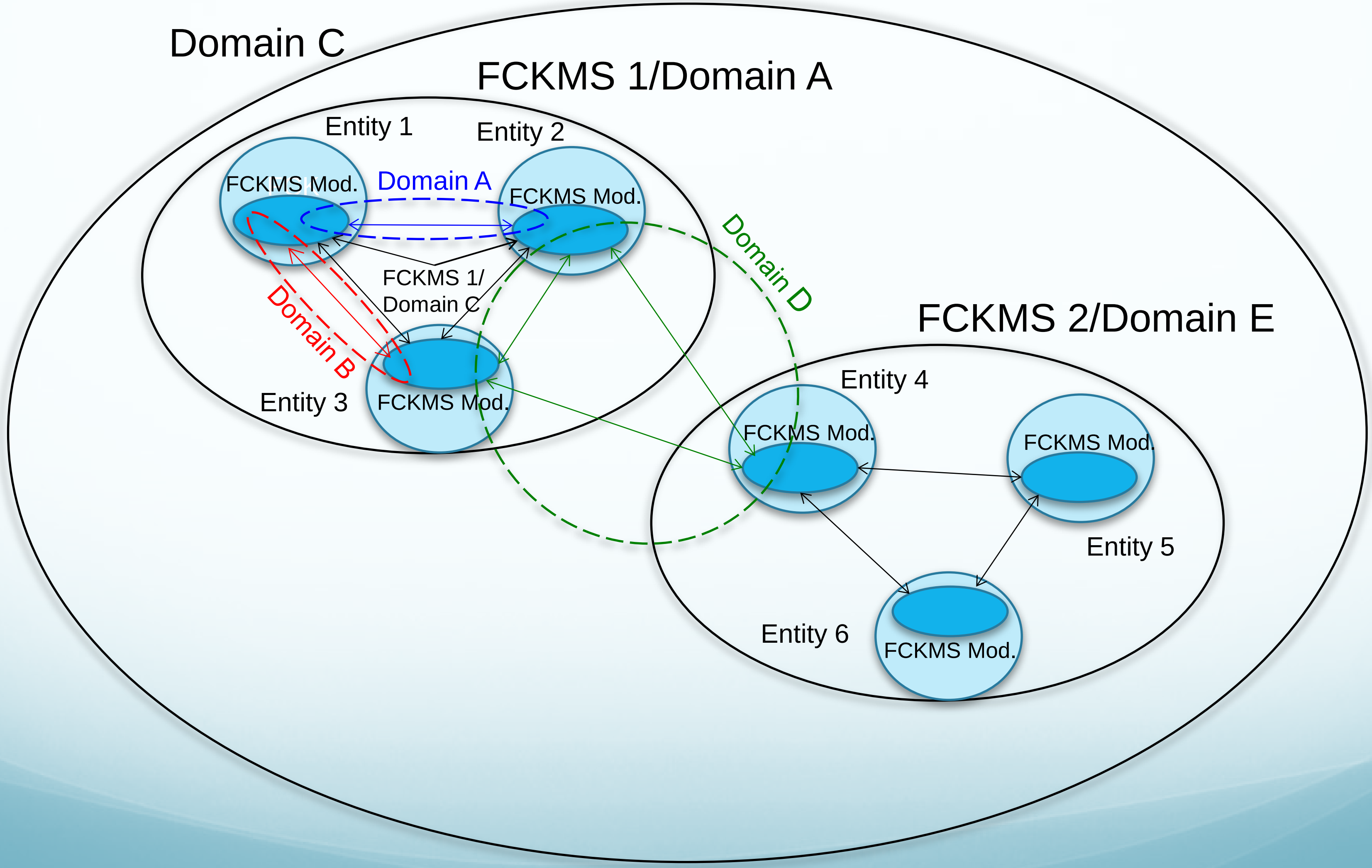
Is Domain Policy {A, B} ≤ FCKMS 1/Domain C Policy?

More FCKMS and Domains

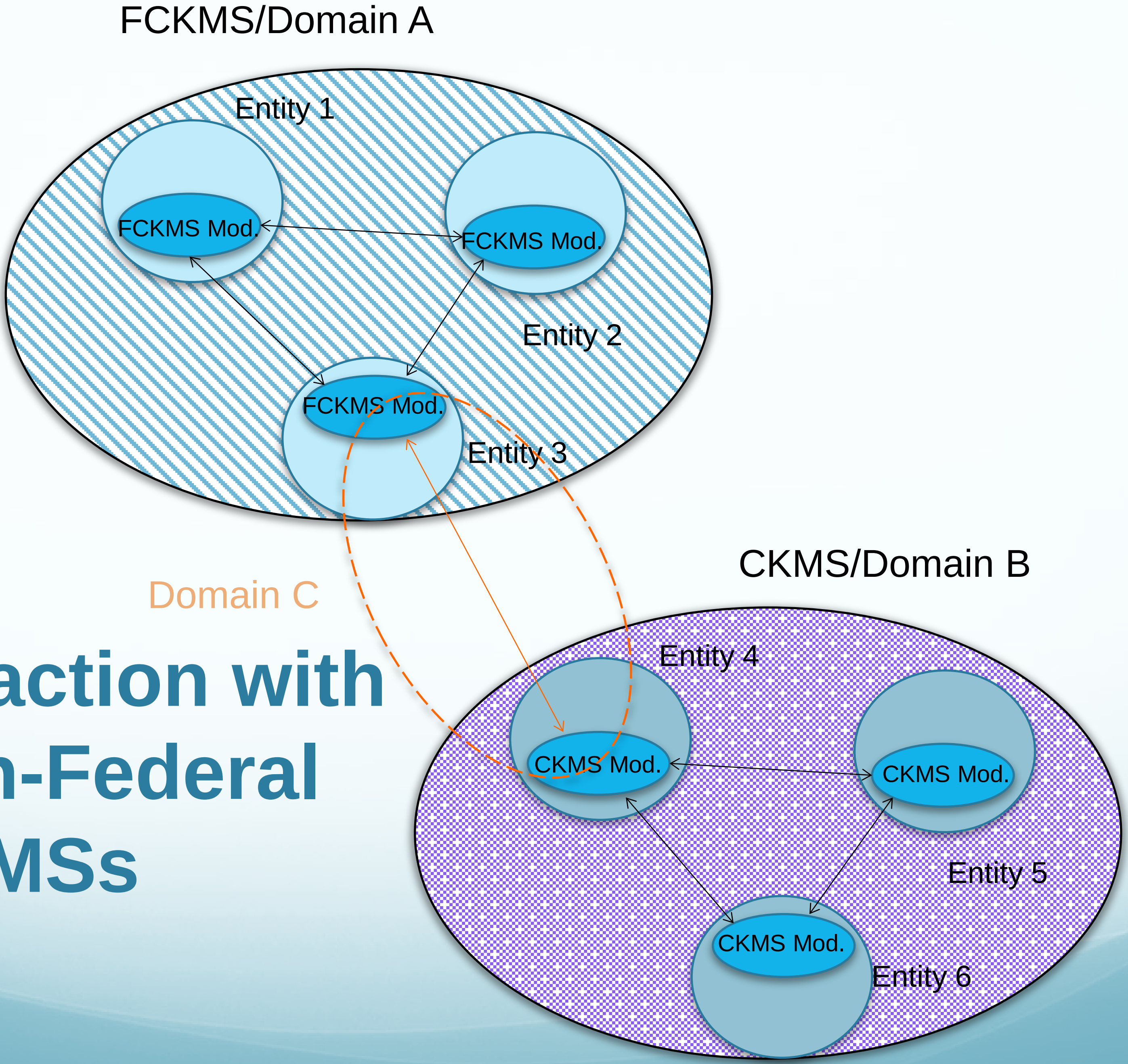


Does FCKMS Policy A =FCKMS Policy B = Domain Policy XYZ?
Can FKMS Policy {A, B} ≤ Domain Policy XYZ?
Can FCKMS Policy A ≠ FCKMS Policy B?

Multiple FCKMSs and Domains



Interaction with Non-Federal CKMSs



Domain Security Policy
(Section 4.4.1)

- Derived from the Information Management and Security policies of all organizations working together in the security domain.
- No sharing between domains unless equivalence of compatibility is determined.
- An FCKMS module could support multiple Domain Security Policies and keep the keys separate.
- A domain could consist of multiple FCKMSs or an FCKMS could support multiple domains.
- A Domain Security Policy is recommended in PA: 4.4.
- Who is responsible for the policy? The FCKMS service providing org. or service using org. or both?

Questions and Comments?

Roles and Responsibilities

(Section 5)

Dennis Branstad

FCKMC Roles and the People who Perform Them

- An FCKMS includes roles specified by its authorities that **could** be filled by one or more people who are performing specific administration, management, operational, and user duties.
- Each **role could be performed** by one or more people.
- Each **person could perform** one or more roles (except for the FCKMS Auditor Role – see **PR:5.3**).

FCKMS Defined Roles

- **Authorities**: System Authority and Domain Authority.
- **Administrators**: System Administrator and Audit Administrator.
- **Operations Personnel**: Registration Agent, Key-Recovery Agent, Key Custodian, Cryptographic Officer, and CKMS Operator.
- **Users**: Key Owners and FCKMS users.
- **Other Roles**: Could be defined as needed.

Required FCKMS Roles and Responsibilities (PR:5.1)

- **System Authority:** Senior Federal official responsible for an FCKMS, including its Security Policy, Procurement, Administration, Management, and Operation Authorization.

- **System Administrator**: Federal official responsible for FCKMS management, security, operation, and maintenance.

- **Audit Administrator**: Federal official responsible for assuring that all Roles are performed by authorized individuals, collecting security relevant information, and preparing audit reports for the System Authority and System Administrator.

- **User**: A Federal organization, employee, or contractor that initiates and uses FCKMS key-management services and functions after being registered and authorized.

FCKMS Role Recommendations and Suggestions

- **PA:5.1** A Federal CKMS **should** support the roles of Cryptographic Officer, Key Custodian, and Key Owner.
- **PA:5.2** Other than the user role, the roles performed within a Federal CKMS **should** be **rotated** periodically **among authorized pers**onnel.
- **PF:5.1** A Federal CKMS **could** support the roles of Domain Authority, Registration Agent, Key-Recovery Agent, and FCKMS Operator.

In Addition -

- **PR:5.2** A Federal CKMS **shall** verify the authorization of the individual initiating one or more activities while performing a role, and restrict the activities of the person performing the role to those allowed by the specification of the role.

Questions and Comments?