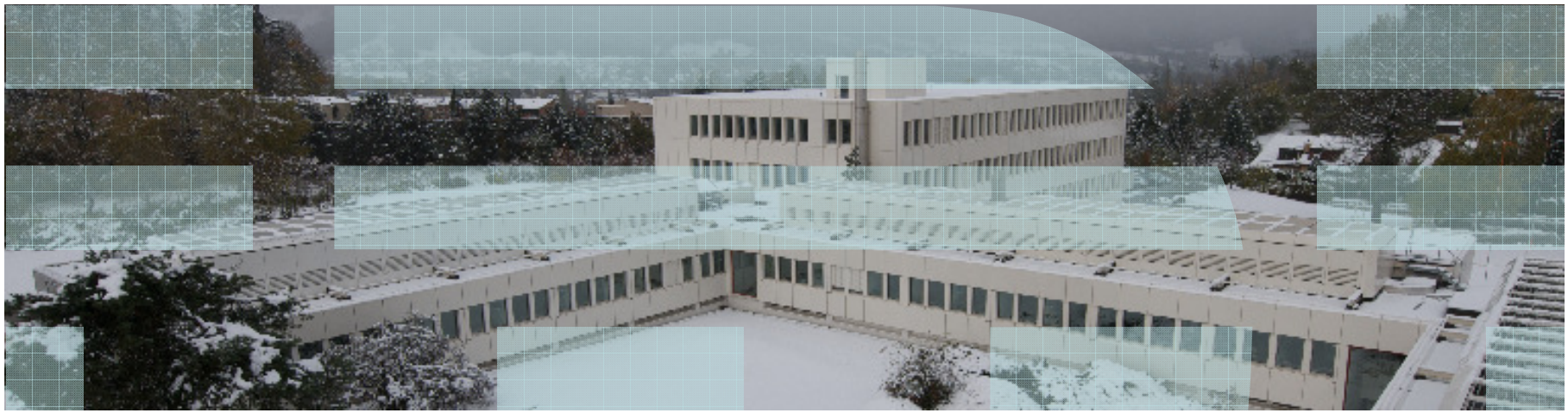
Robert Haas, Marko Vukolić (IBM)

1 September 2010

Access Control in KMIPv1.1



Summary of Changes (wrt. last version of the AC proposal)

- Roles and Access Control List Attribute are removed from the proposal
- The new KMIP v1.1 AC proposal contains:
  - Owner Attribute
  - Operation Policy Properties Attribute
  - Extensions of Link Attribute

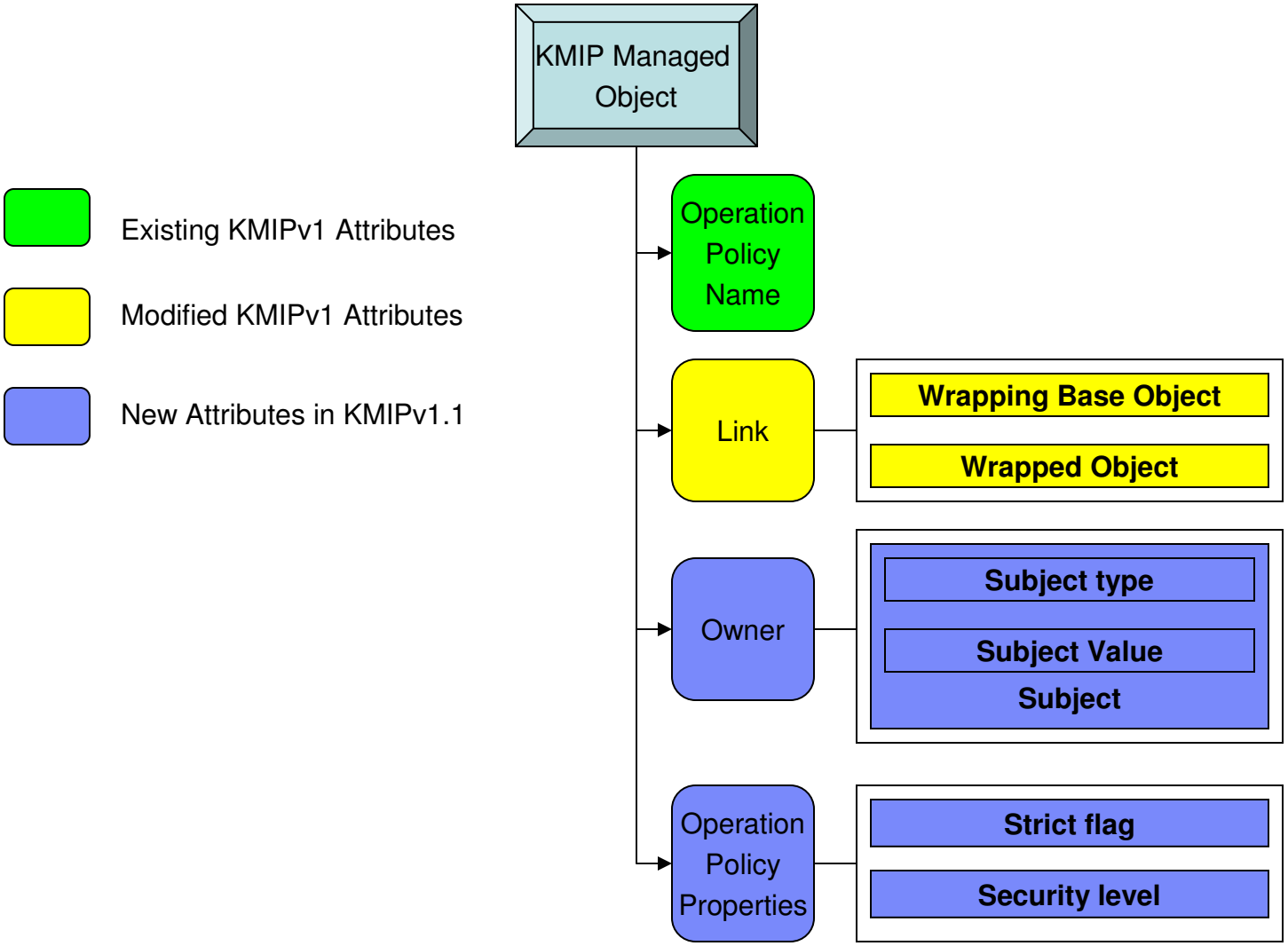
Removal of Roles, Access Control Lists. Why?

- Fears that KMIP server might hold redundant and conflicting information to that already maintained by an external AC infrastructure in a large organization. Potential difficulties in internal vs. external AC parameters synchronization.

- Defining AC in KMIP may become troublesome in case of different administrative/security domains (with e.g., different roles, different policies applicable to different servers).

- This new proposal recommends to:
  - Handle access control decisions and permissions via an external AC infrastructure, out of the scope of the KMIP specification
  - Define a minimal yet sufficient support in KMIP for **object ownership** and **strict access control**

Current Proposal Overview



Link

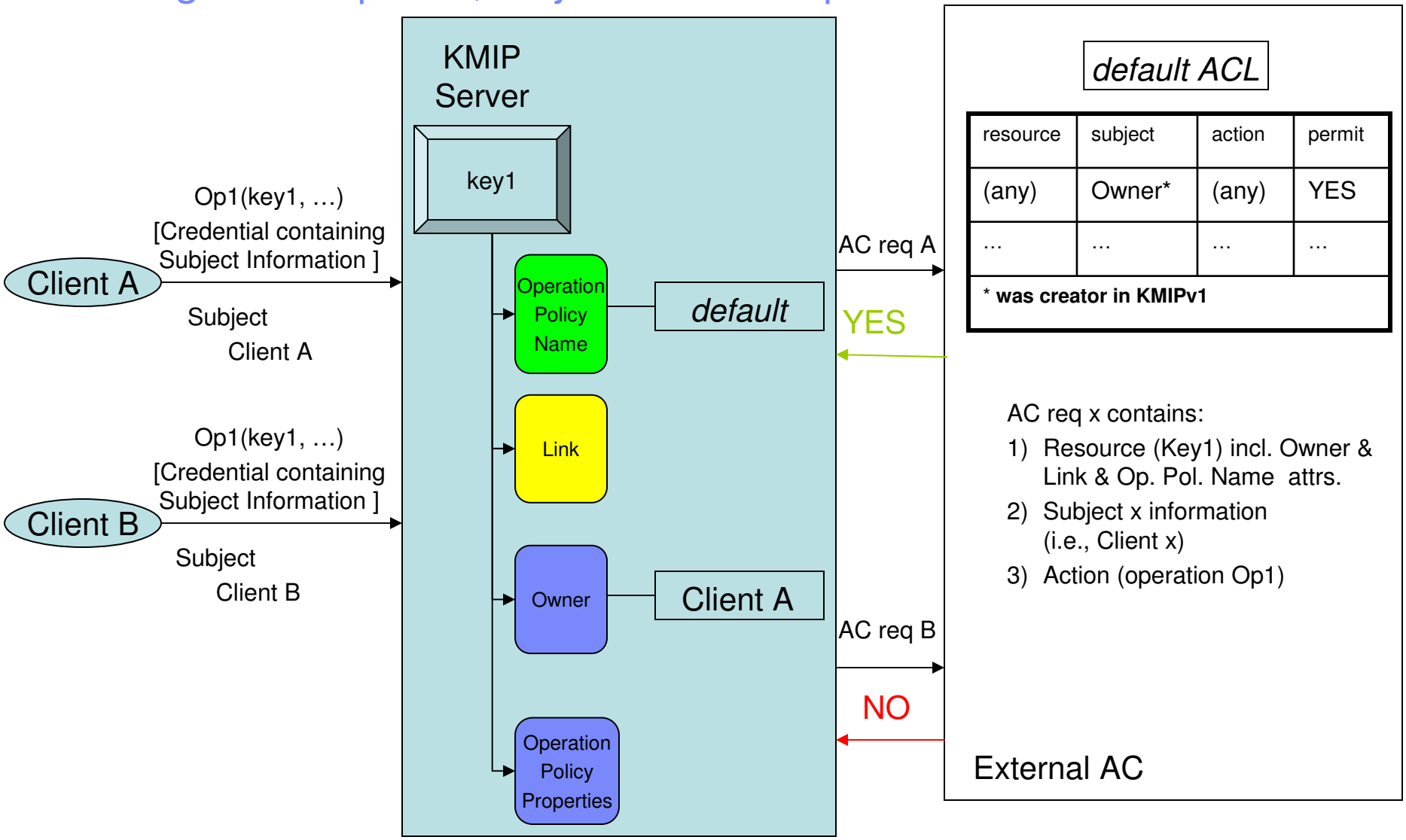
- Introduce New Link Types to allow KMIP server to track dependencies among keys
- Needed for Strict AC that protects against KMIP API attacks that exploit dependencies
- Tracking dependencies unrealistic to be deferred to an external AC
  - KMIP server should do it and hence enable Strict AC Policy (not specified in protocol) to be enforced externally
- **New Link Types**
  - ***Wrapping Base Object Link:*** for an object specified in Key Wrapping Data and used to wrap current object in Get operation
  - ***Wrapped Object Link:*** the object that was wrapped using the current object.
- Derivation dependencies already tracked in KMIPv1

Owner

Managed Object Attribute	Encoding	REQUIRED
Owner	Subject	YES

SHALL always have a value	Yes
Initially set by	Server
Modifiable by server	Yes
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Re-key, Certify, Re-Certify
Applies to Object Types	All Objects

Handling AC Requests, Object Ownership



KMIP v1.1: By default, Owner SHALL be the creator of the object

Subject

Object	Encoding	REQUIRED
Subject	Structure	
Subject Type	Enumeration, see below	Yes
Subject Value	Varies.	Yes

Subject type enumeration

Subject type	
Name	Value
Username	00000001
Device	00000002
World Wide Name	00000003
Distinguished Name	00000004
SAML Subject	00000005
WS Security Token	00000006
openID	00000007

Subject Values

Subject type	Subject Value		
	Object	Encoding	REQUIRED
Username	Subject value	Text String	YES
Device	Subject value	Structure	
	Device Serial Number	Text String	YES
	Device Group	Text String	NO
	Device Text	Text String	NO
	Host Machine ID	Text String	NO
	Host Machine Text	Text String	NO
World Wide Name	Subject Value	Text String	YES
Distinguished Name	Subject Value	Text String	YES
SAML Subject	Subject Value	Text String	YES
WS Security Token	Subject Value	Text String	YES
openID	Subject Value	URI	YES

Operation Policy Properties

- A new, optional Managed Object Attribute. Used by the server to the client important operation policy properties that apply to a given object.

Managed Object Attribute	Encoding	REQUIRED
Operation Policy Properties	Structure	NO
Strict Flag	Boolean	NO
Security level	Enumeration (FIPS 140-2)	NO

SHALL always have a value	No
Initially set by	Server
Modifiable by server	Yes, Strict flag can never be modified to true
Modifiable by client	No
Deletable by client	No
Multiple instances permitted	No
When implicitly set	Create, Create Key Pair, Register, Derive Key, Re-key
Applies to Object Types	All Objects

Next steps

- Synchronize Credential and Subject fields