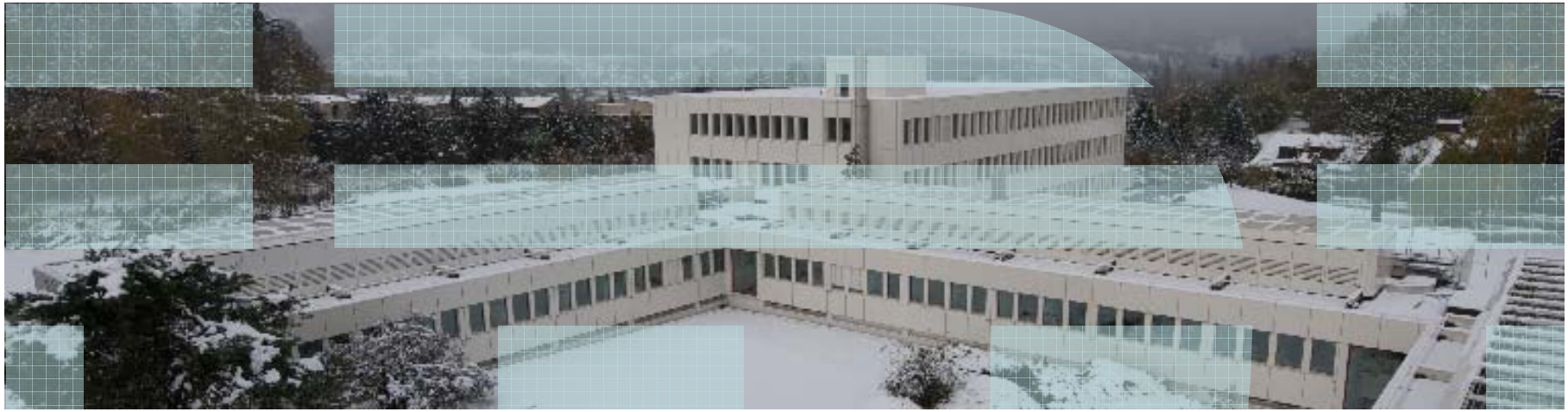
Robert Haas (IBM)

Feb 18, 2011

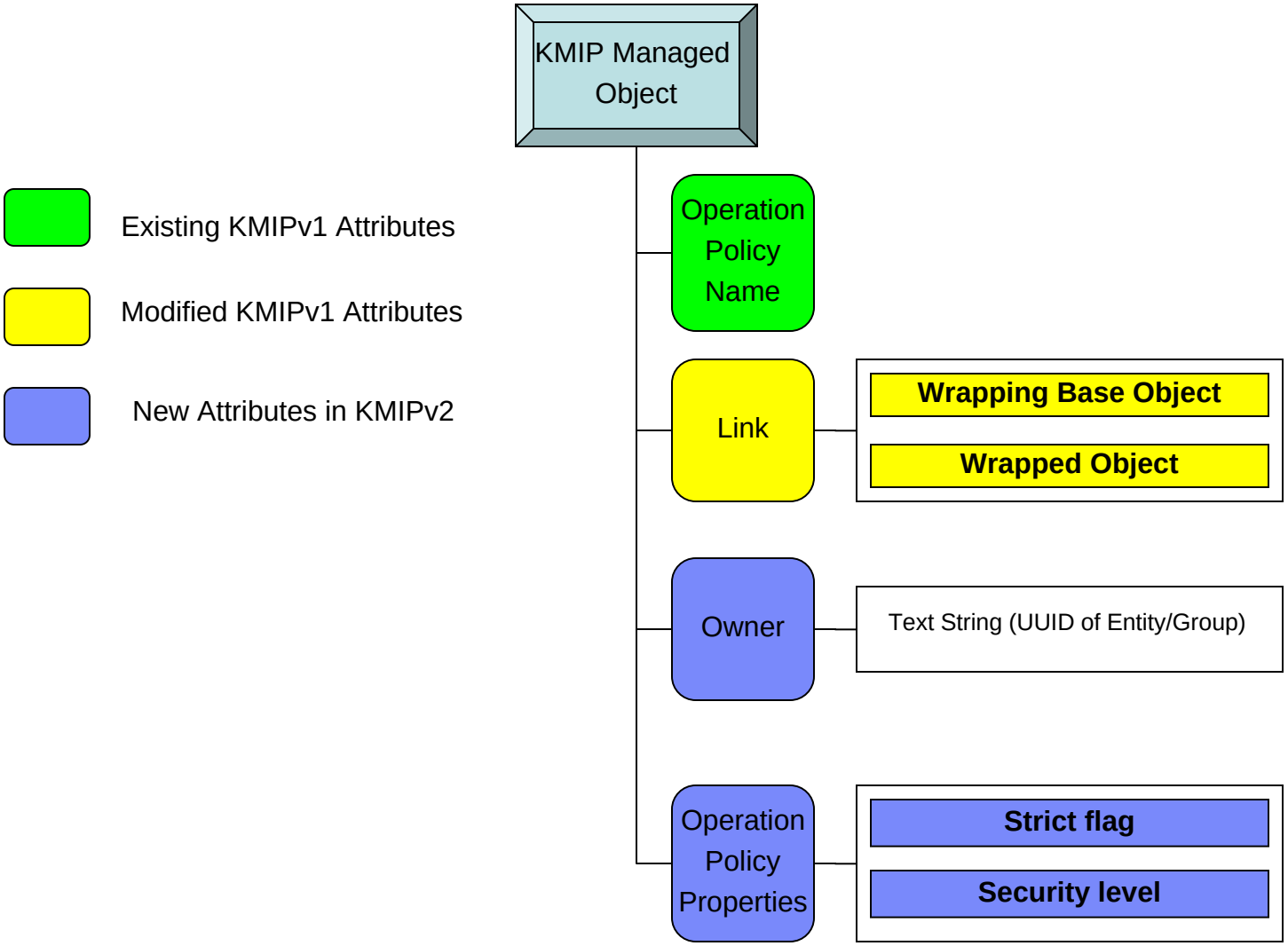
Access Control in KMIPv2



Summary of Changes (wrt. version of the AC proposal from Sep 29 2010)

- Introduction of Entity object and Owner attribute

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

Operation Policy Properties

- A new, optional Managed Object Attribute. Used by the server to tell 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

Example