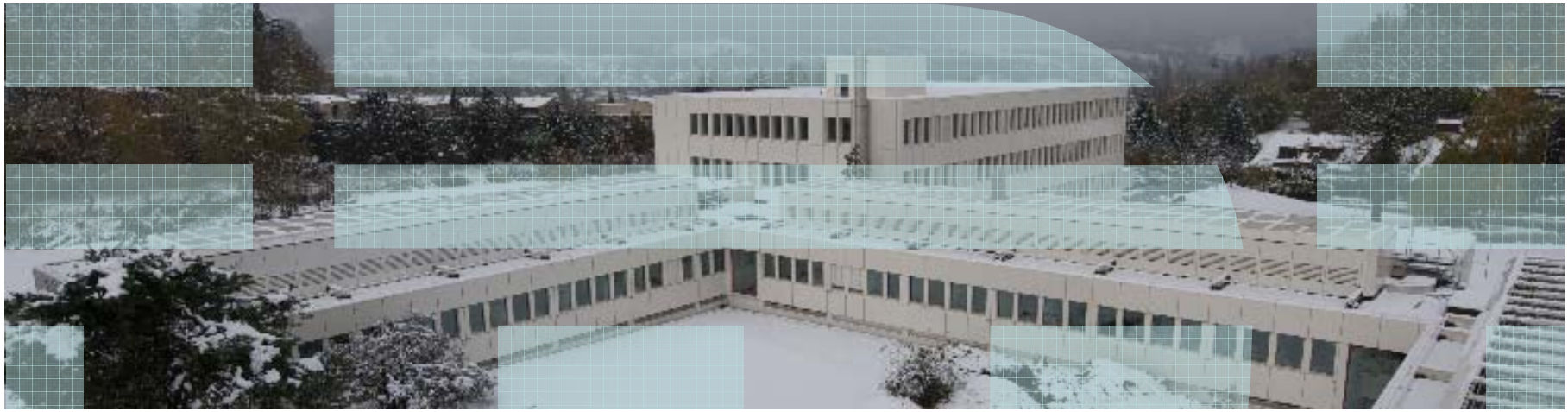
Robert Haas <rha@zurich.ibm.com>

September 28 2009

# Server-to-server (s2s) in KMIPv2 (or v1.x)



# Outline

- Server-to-server (s2s) use cases
- Deficiencies of KMIPv1 for s2s
- Concerns for s2s support in KMIPv2

# Server to server (s2s) use cases

- Backup
- Load balancing/Delegation
- Propagating key material closer to endpoints, e.g.,
  - Example 1 (A retail store)
    - A retail store operation with each store relying on encrypted storage
    - network connectivity with the central key management server (CKMS) not reliable
    - small subset of the keys needed to be served locally, but the management is at CKMS
    - Keys at local key-management servers could be read-only, with pre-allocated usage or lease time
    - The local server needs to communicate with the CKMS
  - Example 2 (e-commerce websites)
    - Multiple e-commerce websites centrally managed (CKMS)
    - Some keys need to be pushed down from CKMS (readable locally), i.e., with CKMS exporting the keys
- Propagating key material updates towards the central key manager
  - A large multinational bank needs the information about cryptographic material from Location B in central Location A (but not vice versa)

# Server to server (s2s) use cases (cnt'd)

- Business-partner data exchange
  - Propagation of keys between KMIP servers to facilitate business partner data exchange
- Partitioning and M&A
  - A KMIP server needs to be partitioned into more servers
  - A company acquires another and cryptographic objects from different KMIP servers need to be merged
- KMIP server acting as the gateway/proxy
  - A less capable KMIP server may need to proxy client's request to the more capable KMIP server (e.g., to interact with a PKI)
- Replication (fault-tolerance)
- Exchange of different server policies and their enforcement

# Additional use cases?

- Suggestions?