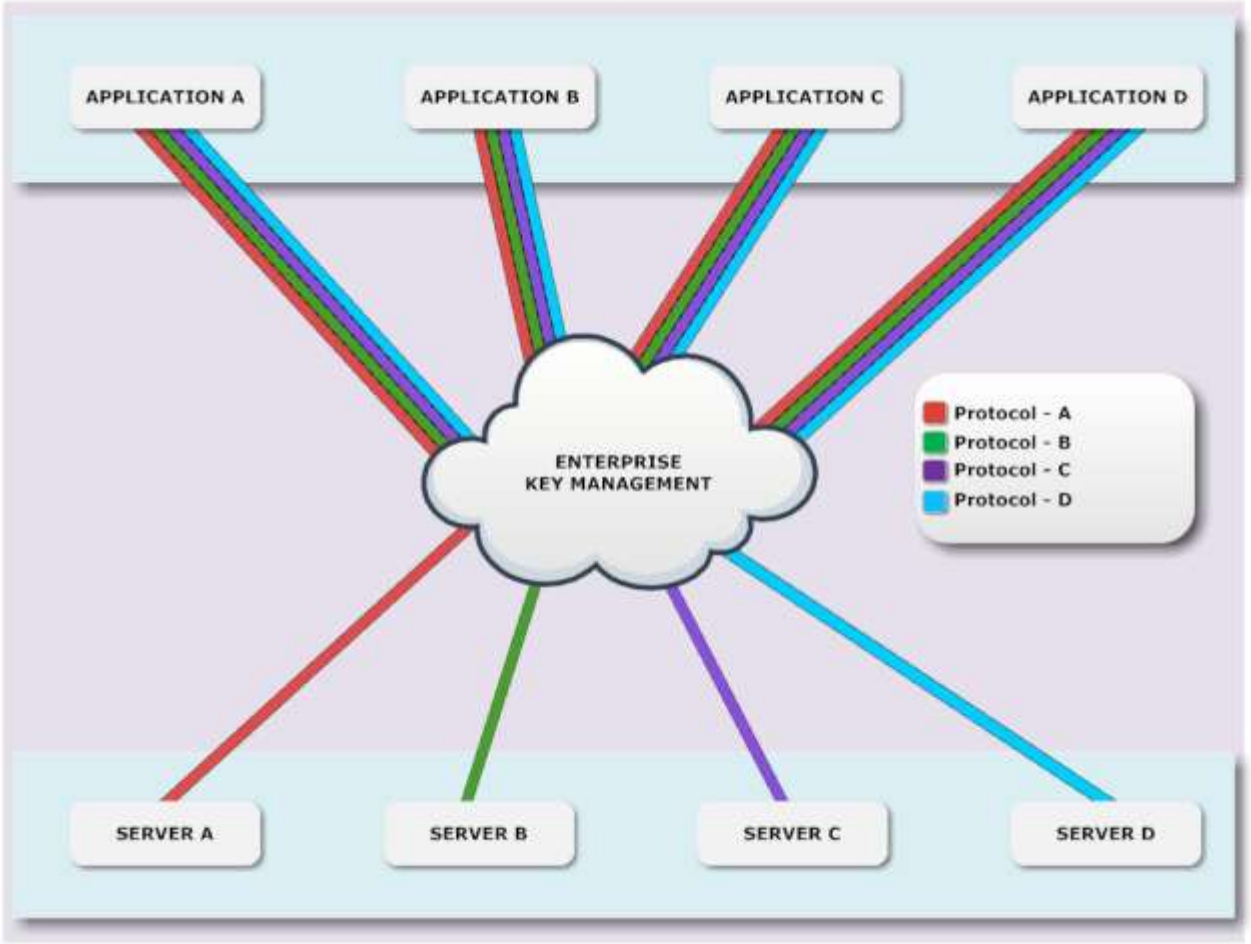
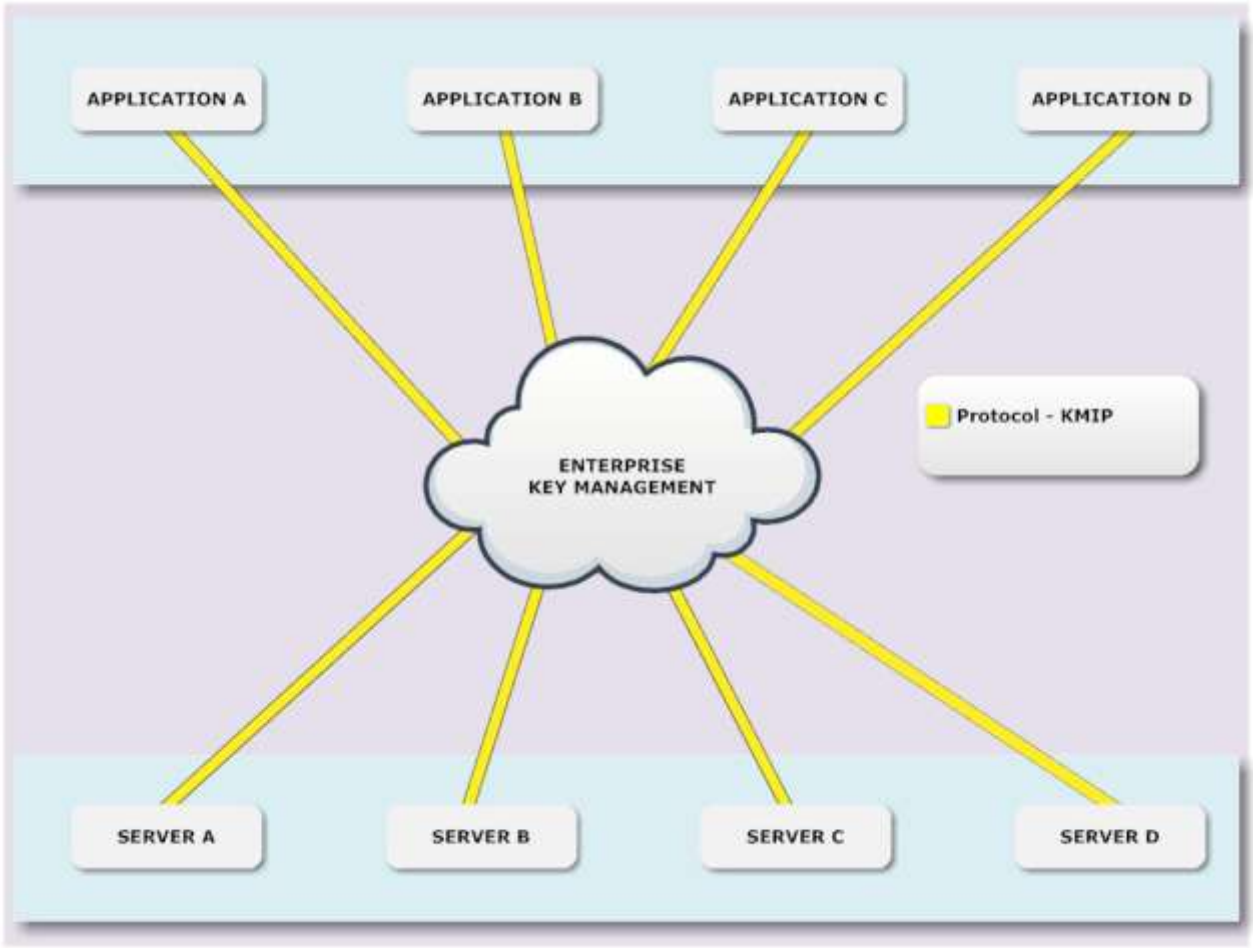
Key Management Interoperability Protocol (KMIP)

Interoperability Demonstration

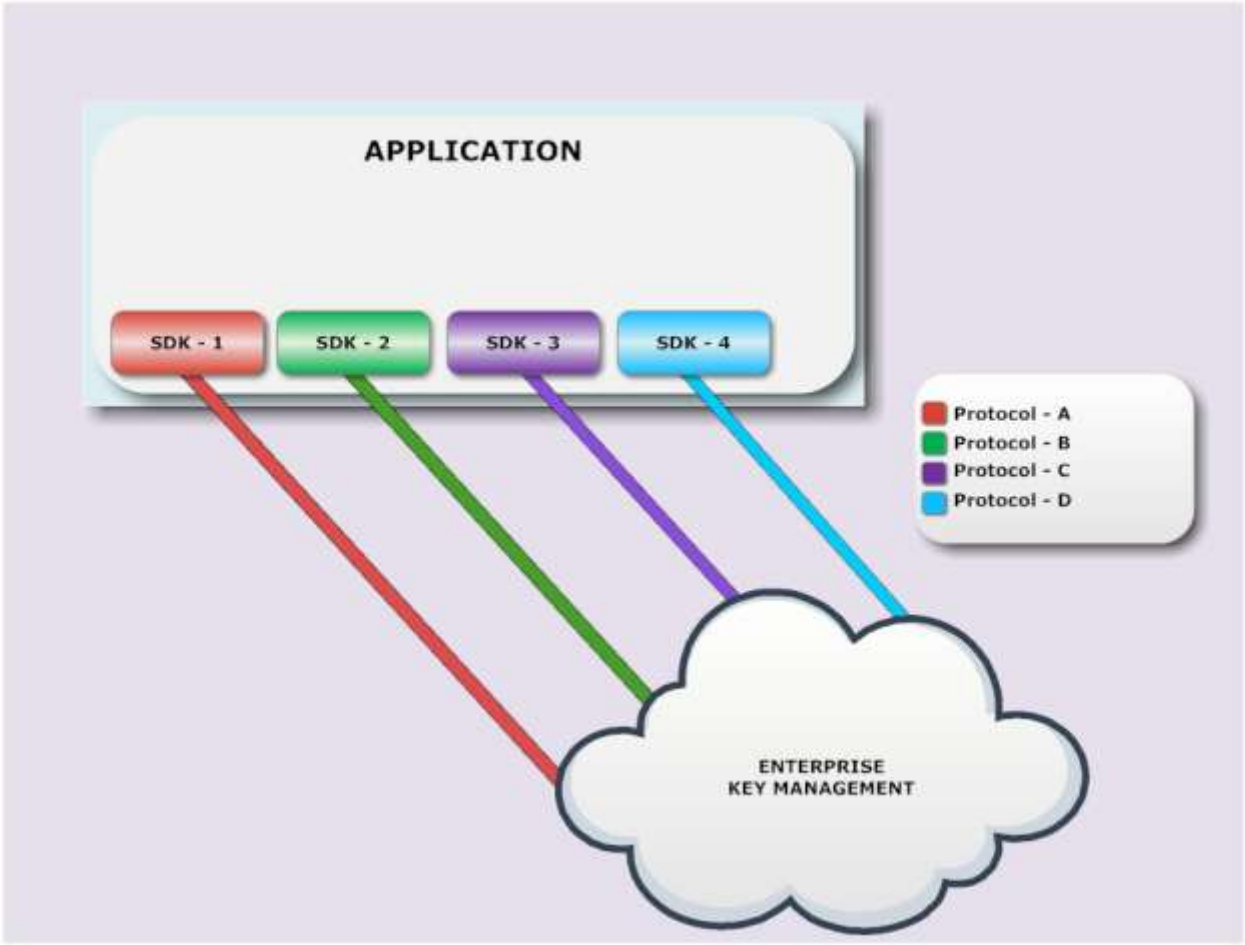
Prior to KMIP each application had to support each vendor protocol



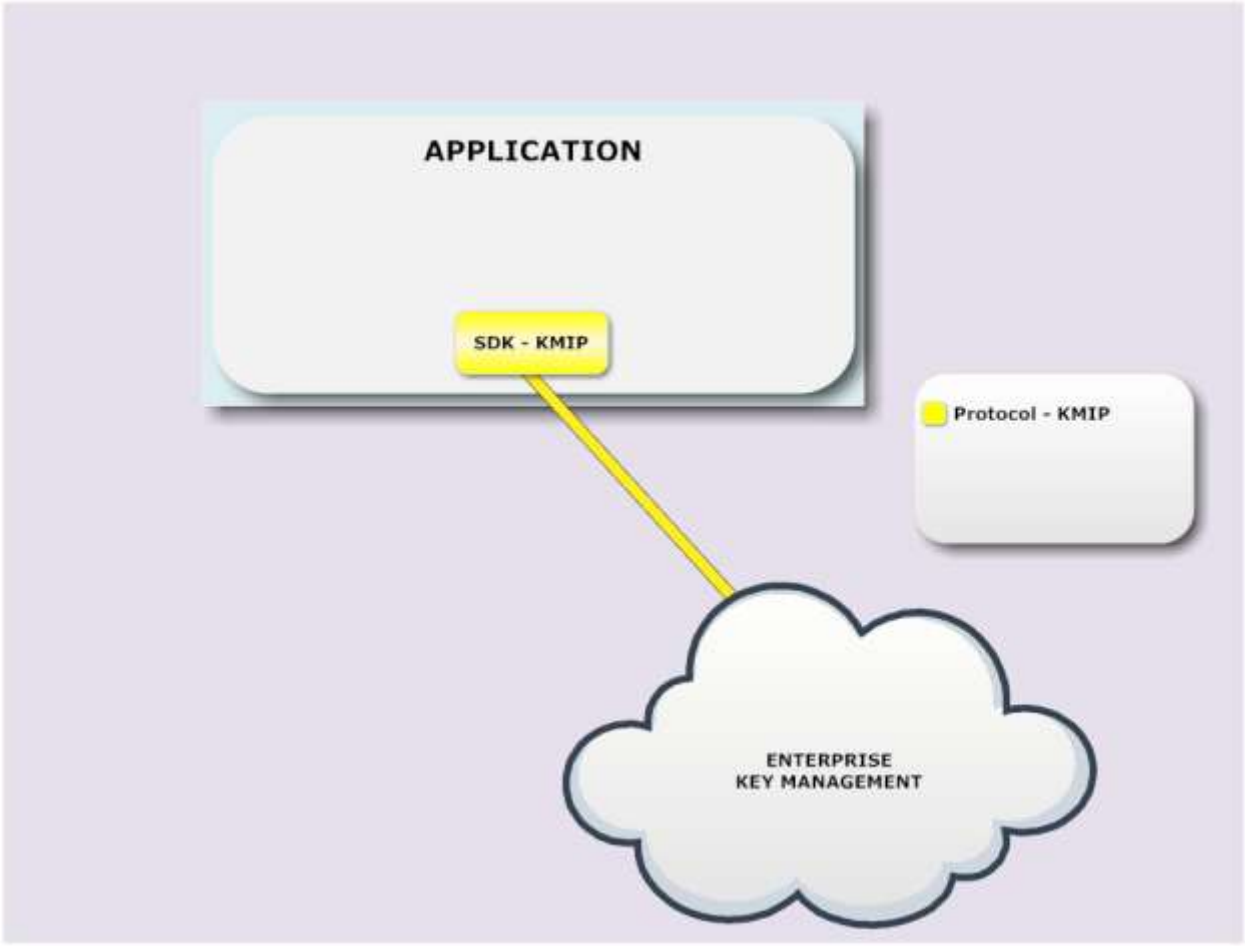
With KMIP each application only requires support for one protocol



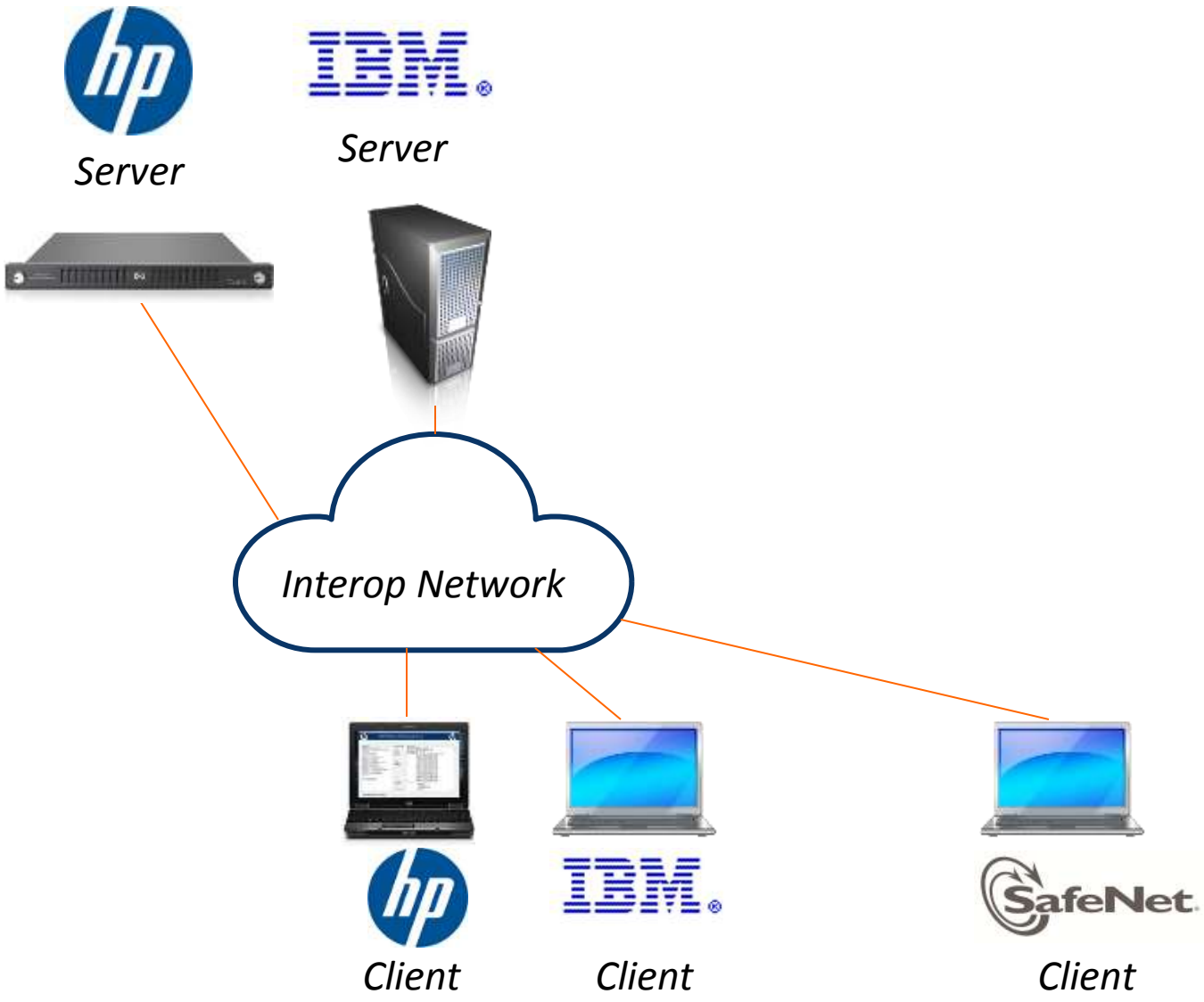
Prior to KMIP each application had to integrate each vendor SDK



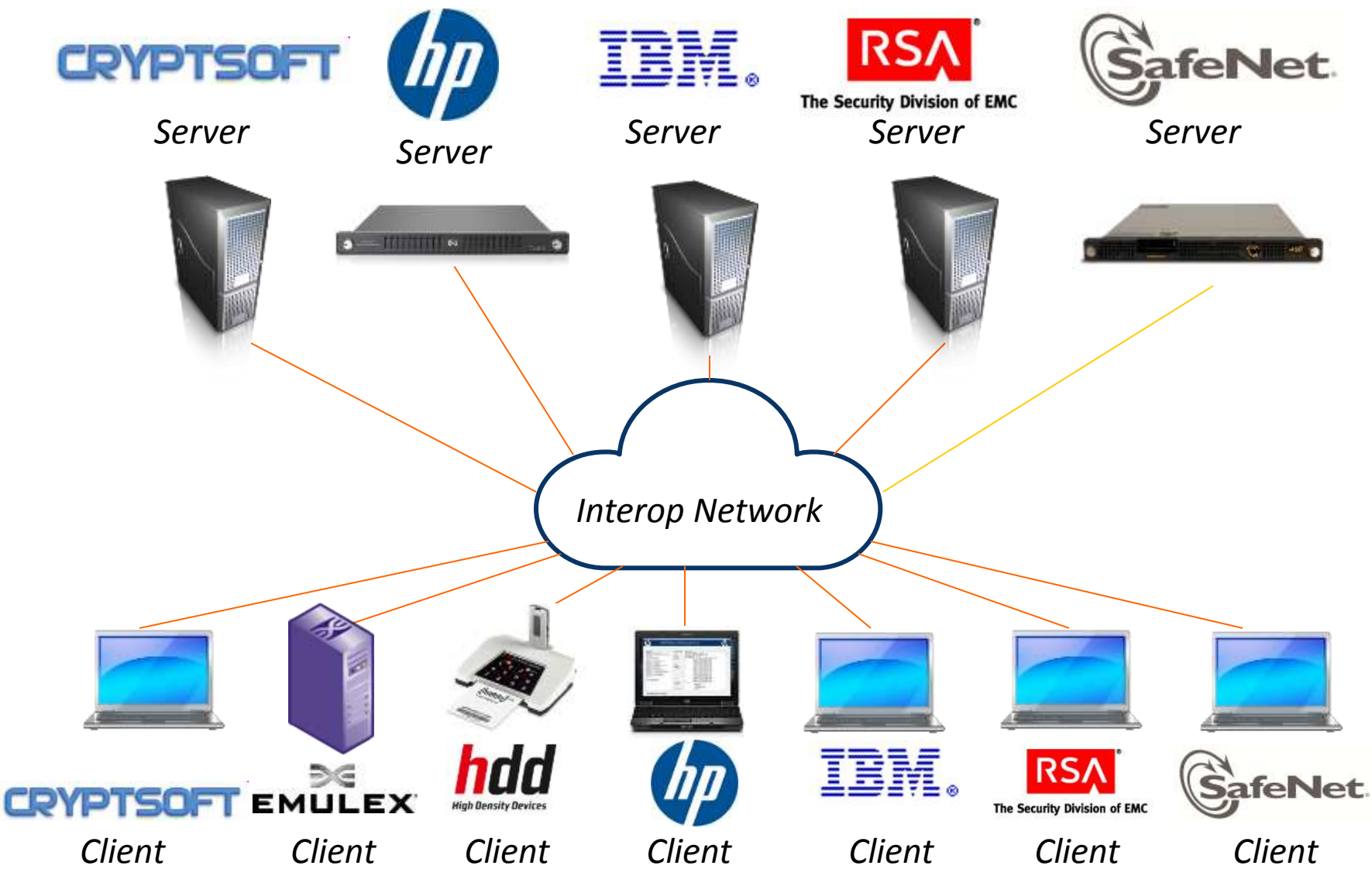
With KMIP each application only requires one vendor SDK integration



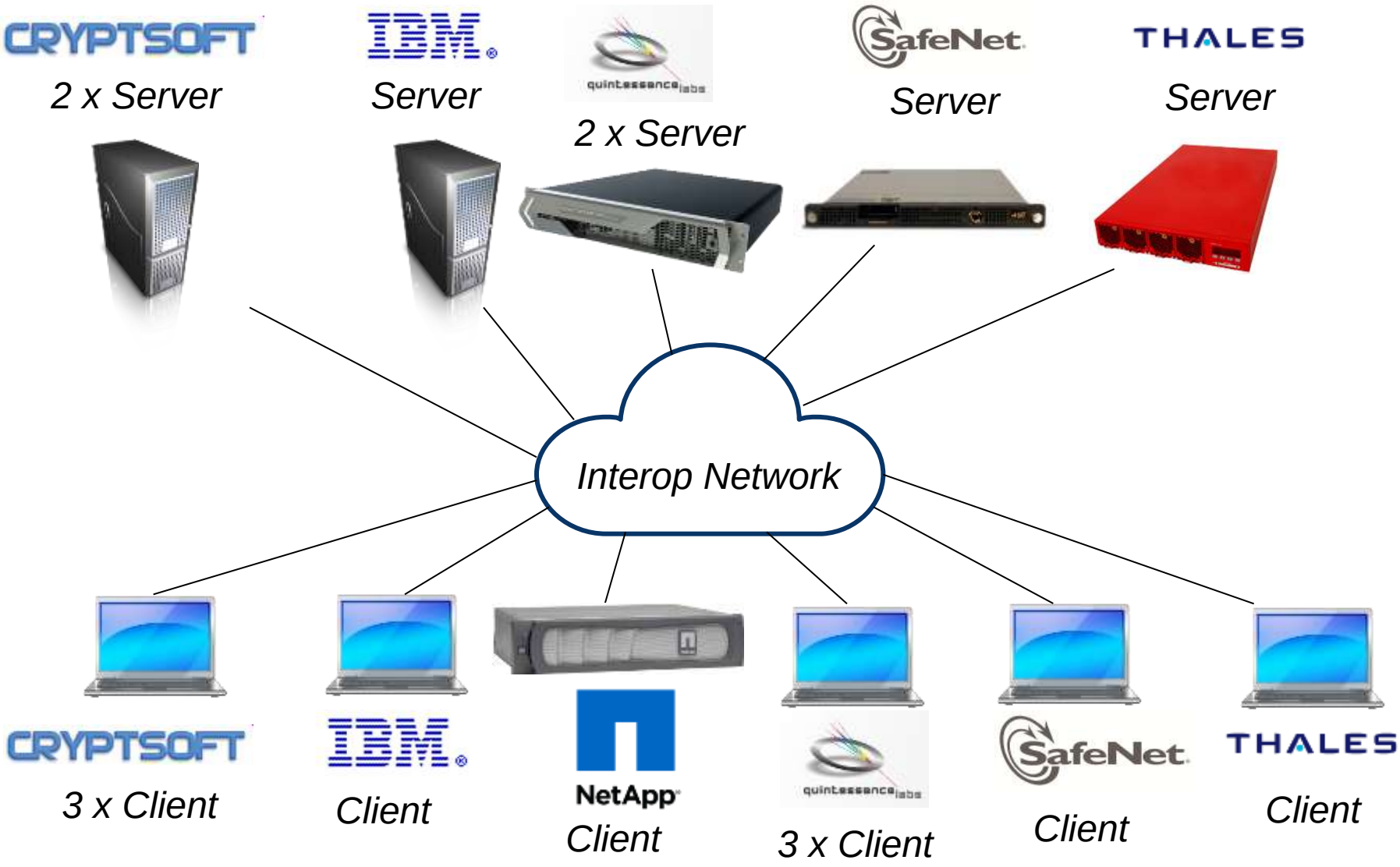
2010



2011


CRYPTSOFT
Server
Server
IBM
Server
RSA
The Security Division of EMC
Server
SafeNet
Server
Interop Network
CRYPTSOFT
EMULEX
hdd
High Density Devices
IBM
RSA
The Security Division of EMC
SafeNet
Client
Client
Client
Client
Client
Client
Client

2012


CRYPTSOFT
2 x Server
IBM
Server
quintessencelabs
2 x Server
SafeNet
Server
THALES
Server
Interop Network
CRYPTSOFT
3 x Client
IBM
Client
NetApp
Client
quintessencelabs
3 x Client
SafeNet
Client
THALES
Client

Use Cases

3.1.1 - Create / Destroy

3.1.2 - Register / Create / Get attributes / Destroy

3.1.3 - Create / Locate / Get / Destroy

3.1.4 - Dual client use-case, ID Placeholder linked Locate & Get batch

3.1.5 - Register / Destroy Secret Data

3.2 - Asynchronous Locate

4.1 - Revoke scenario

5.1 - Get usage allocation scenario

6.1 - Import of a Third-party Key

7.1 - Unrecognized Message Extension with Criticality Indicator false

7.2 - Unrecognized Message Extension with Criticality Indicator true

8.1 - Create a Key Pair

8.2 - Register Both Halves of a Key Pair

Use Cases

9.1 - Create a Key, Re-key
9.2 - Existing Key Expired, Re-key with Same lifecycle
9.3 - Existing Key Compromised, Re-key with same lifecycle
9.4 - Create key, Re-key with new lifecycle
9.5 - Obtain Lease for Expired Key
10.1 - Create a Key, Archive and Recover it
11.1 - Credential, Operation Policy, Destroy Date
11.2 - Device Credential, Operation Policy, Destroy Date
12.1 - Query, Maximum Response Size
12.2 - Query Vendor Extensions
13.1 - Asymmetric Register PKCS#1
13.2 - Asymmetric Register Certificate
13.3 - Asymmetric Create / Re-Key
13.4 - Asymmetric Register / Certify

Use Cases

14.1 - Key Wrapping using AES Key Wrap and No Encoding
14.2 - Key Wrapping using AES Key Wrap with Attributes
15.1 - Locate a Fresh Object from the Default Group
15.2 - Client-side Group Management
15.3 - Default Object Group Member
16.1 - Discover Versions
17.1 - Handling of Attributes and Attribute Index Values
18.1 - Digests of Symmetric Keys
18.2 - Digests of RSA Private Keys

Q&A