Key Management Interoperability Protocol (KMIP)

September 30, 2009

Federated Key Management Panel

The High Points

The Need for Interoperable Key Management

KMIP Overview

KMIP Message Overview

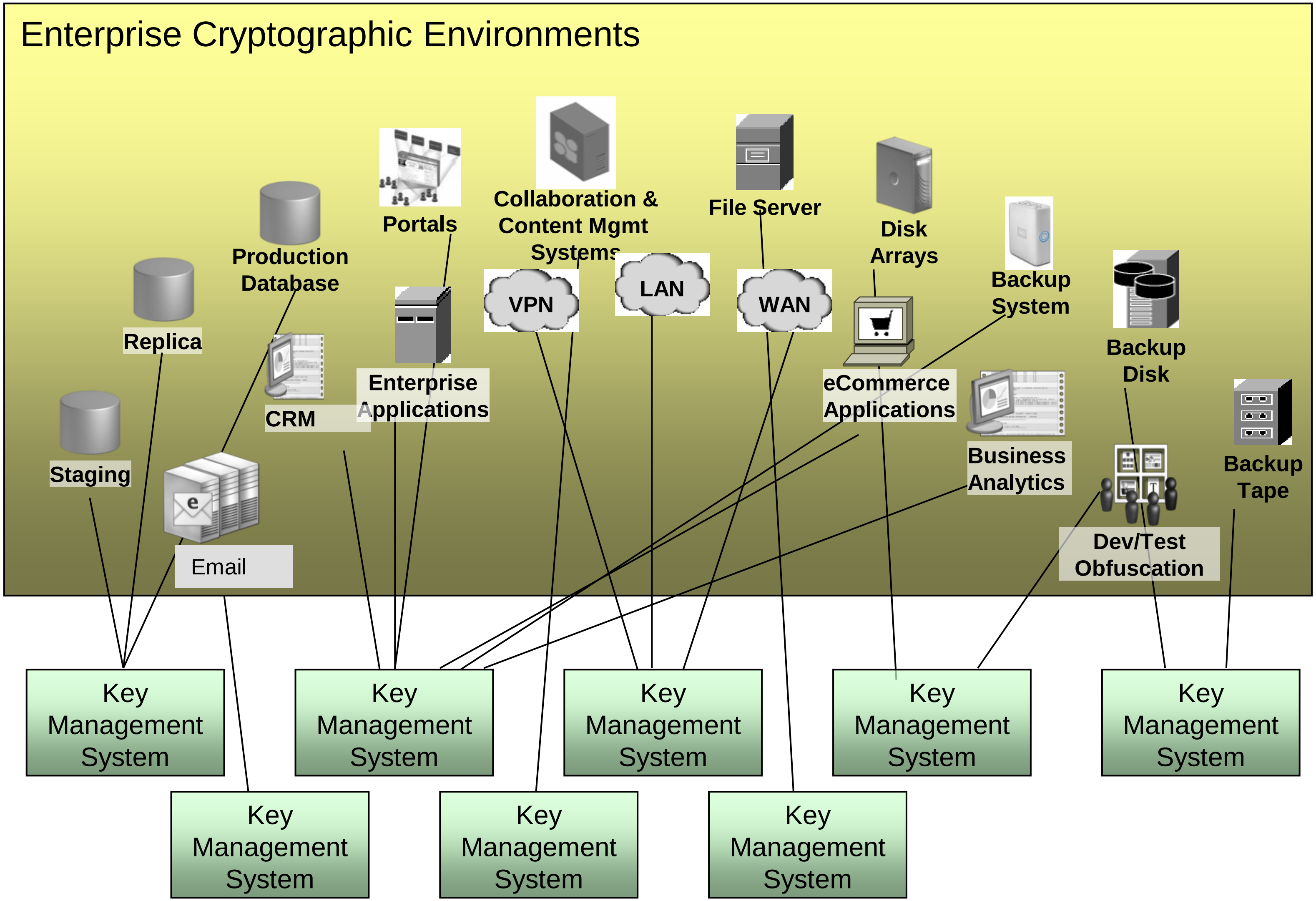
The Need for Interoperable Key Management

- Today's enterprises operate in increasingly complex, multi-vendor environments.
- Enterprises need to deploy better encryption across the enterprise.
- A key hurdle in IT managers deploying encryption is their ability to recover the encrypted data.
- Today, many companies deploy separate encryption systems for different business uses – laptops, storage, databases and applications – resulting in:
    - Cumbersome, often manual efforts to manage encryption keys
    - Increased costs for IT
    - Challenges meeting audit and compliance requirements
    - Lost data

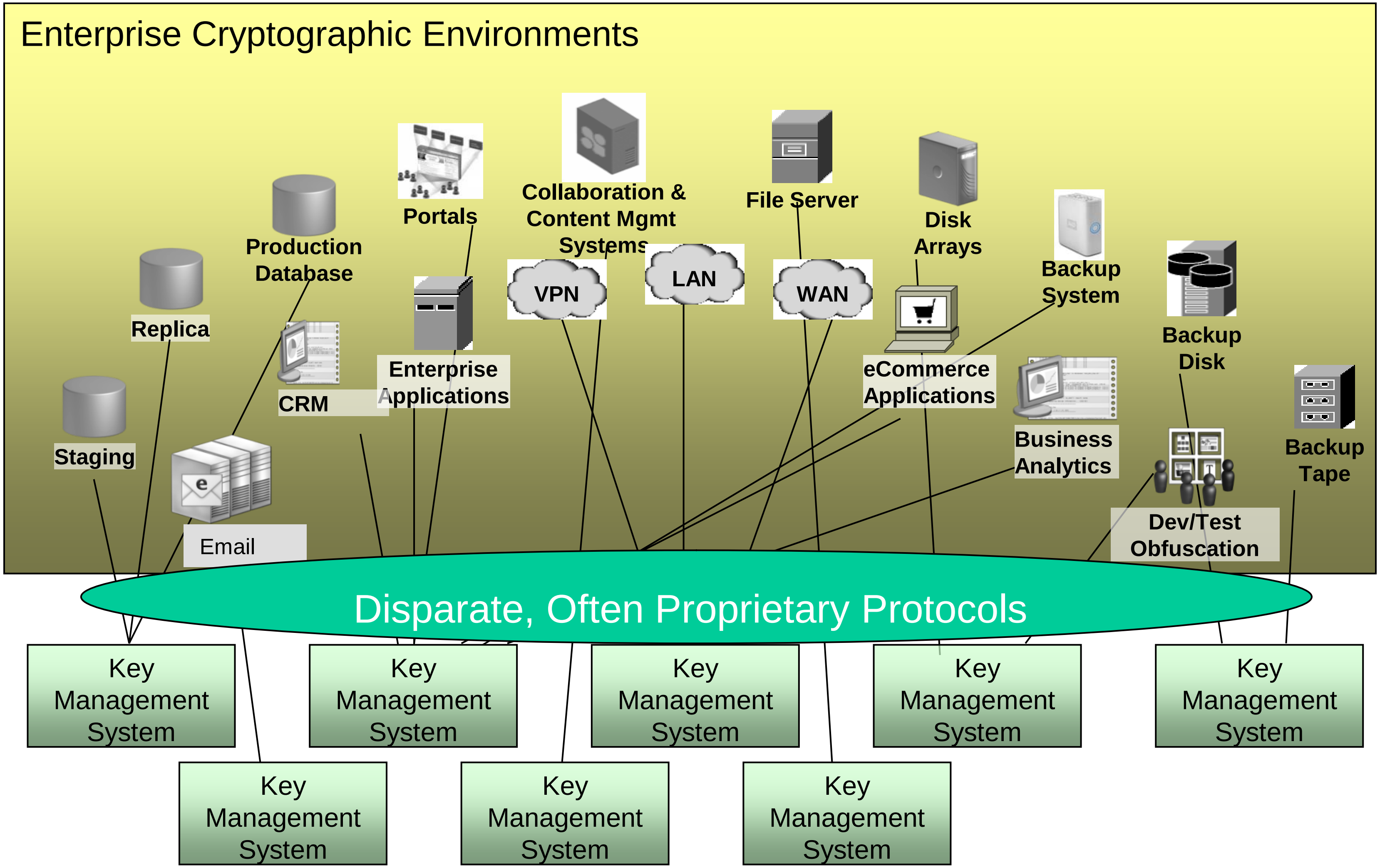
Jon Olstik - ESG

- "As encryption technologies become more pervasive across the enterprise, key management quickly becomes a mission critical activity for protecting the sensitive data. Without a standard way to integrate encryption technologies and key management systems, data confidentiality and integrity may actually degrade. To address this issue, I've long been a strong proponent of key management standards and did what I could to push leading security vendors in this direction. I'm happy to say that the OASIS KMIP effort may finally fill this void."

Often, Each Cryptographic Environment Has Its Own Key Management System

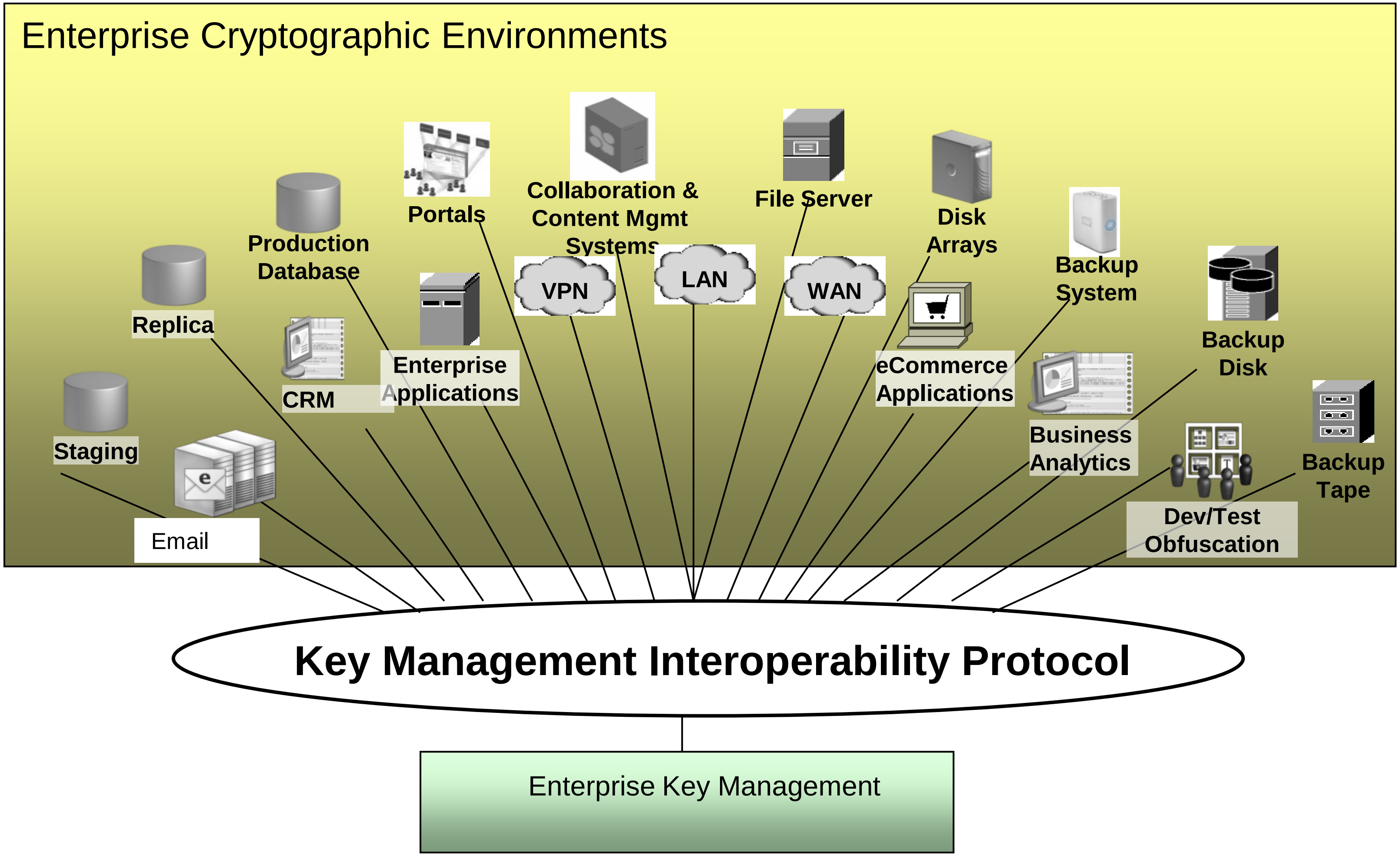


Often, Each Cryptographic Environment Has Its Own Protocol



KMIP Overview

KMIP: Single Protocol Supporting Enterprise Cryptographic Environments



OASIS KMIP Technical Committee

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

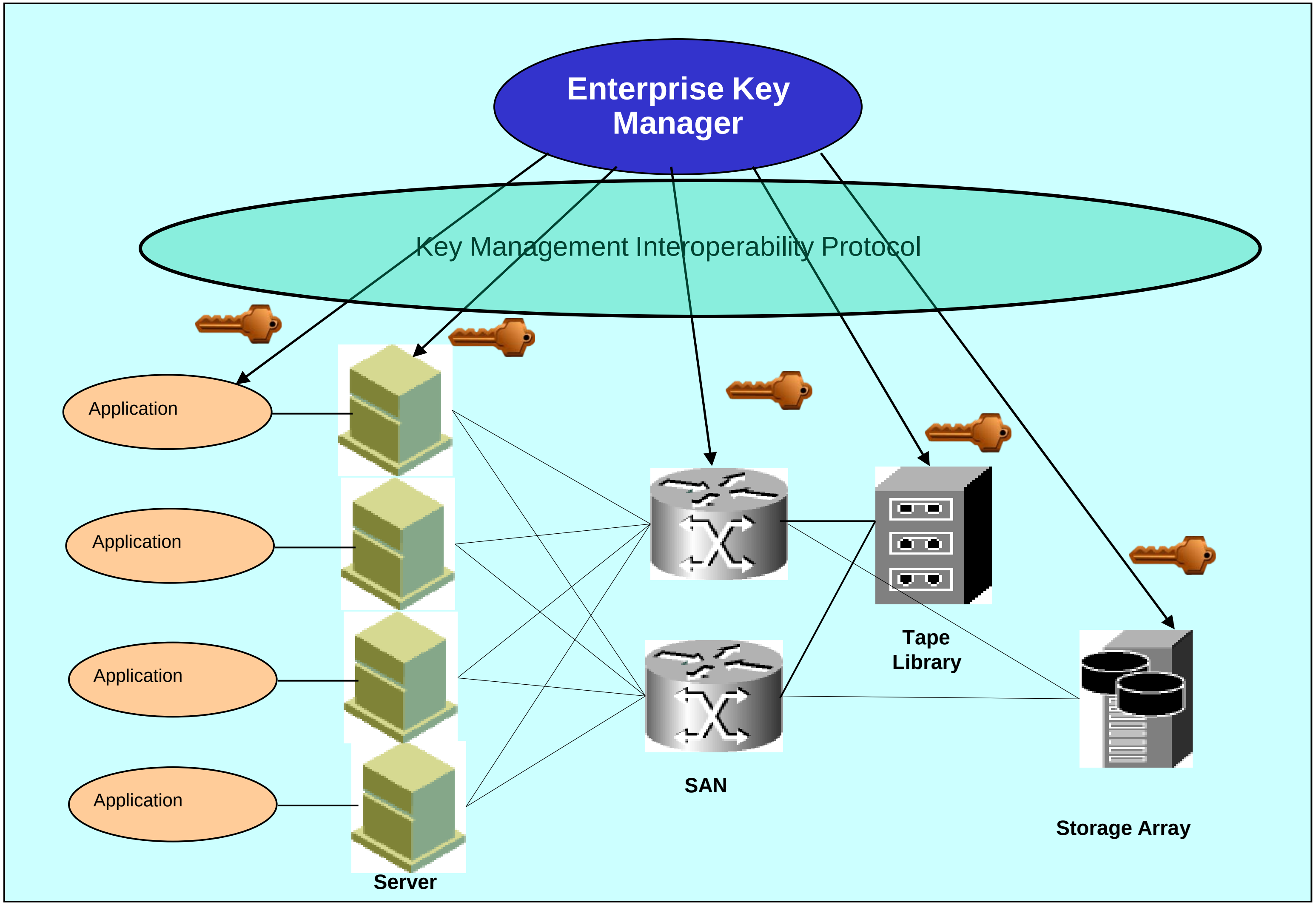
KMIP Technical Committee chartered in March 2009.

> "The KMIP TC will develop specification(s) for the interoperability of Enterprise Key Management (EKM) services with EKM clients. The specifications will address anticipated customer requirements for key lifecycle management (generation, refresh, distribution, tracking of use, life-cycle policies including states, archive, and destruction), key sharing, and long-term availability of cryptographic objects of all types (public/private keys and certificates, symmetric keys, and other forms of "shared secrets") and related areas."

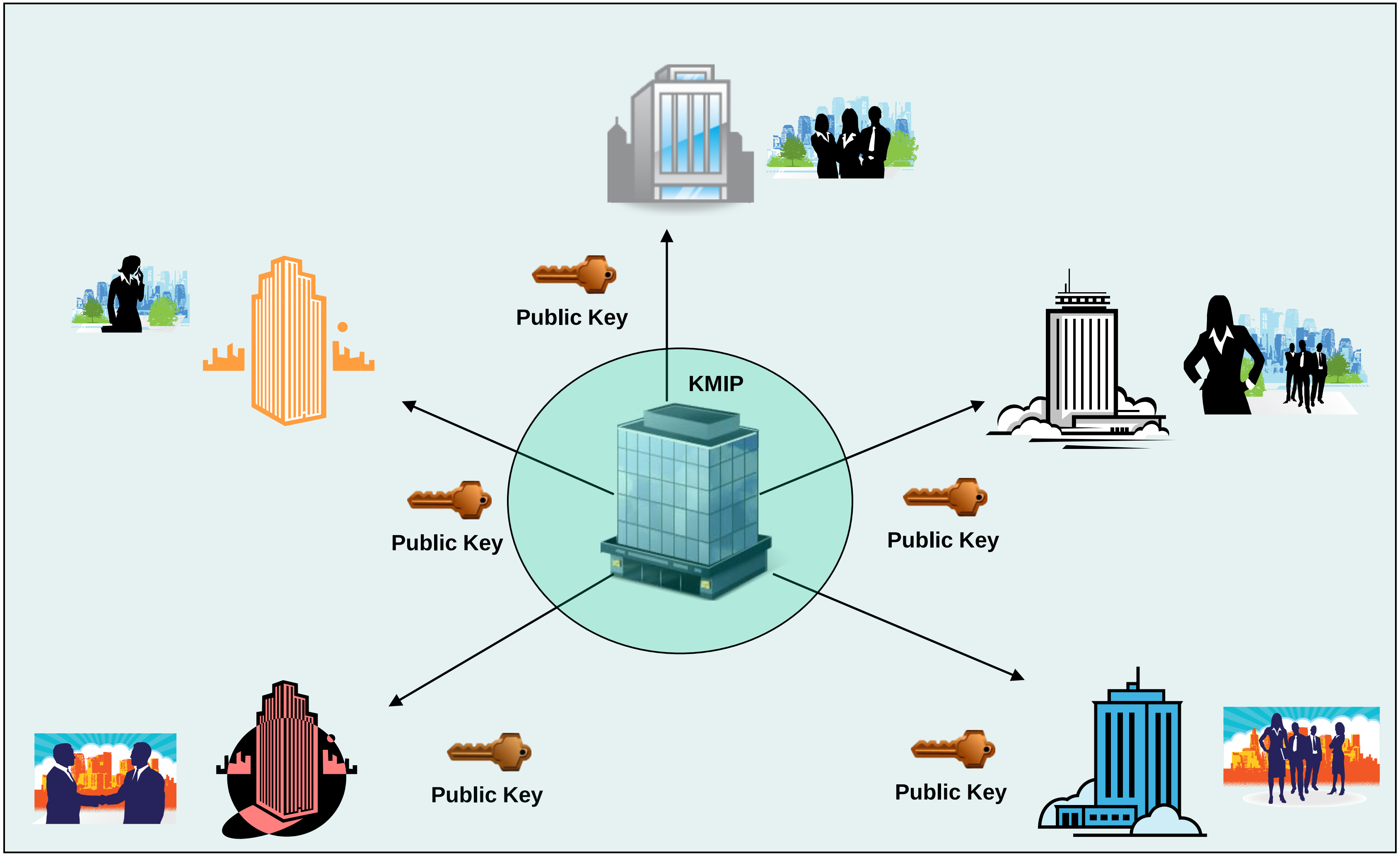
- I.P. mode: "R.F. on RAND"

- Hoping to hit Public Review by EOY 2009

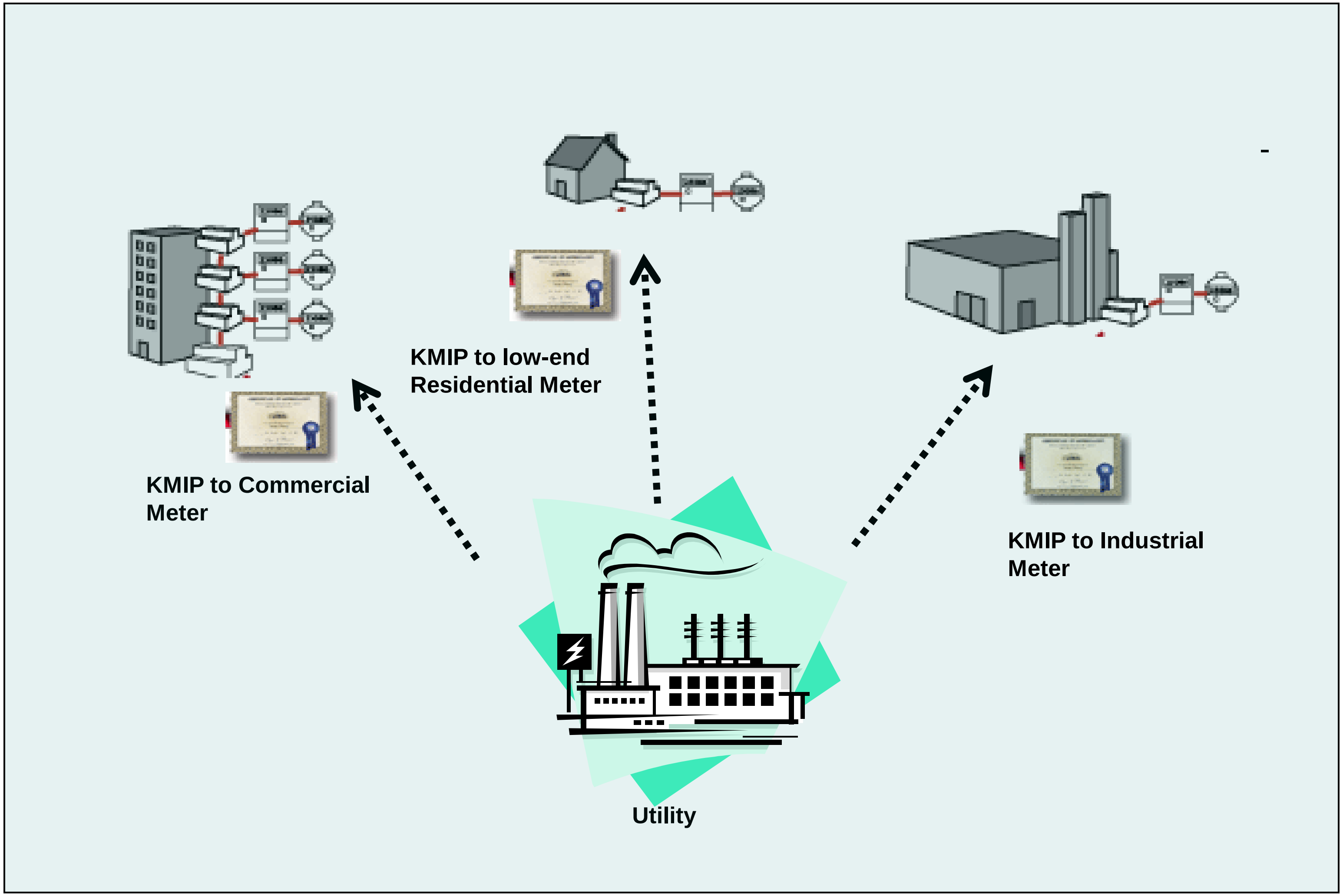
KMIP Objects, Operations and Attributes: Symmetric Encryption Keys



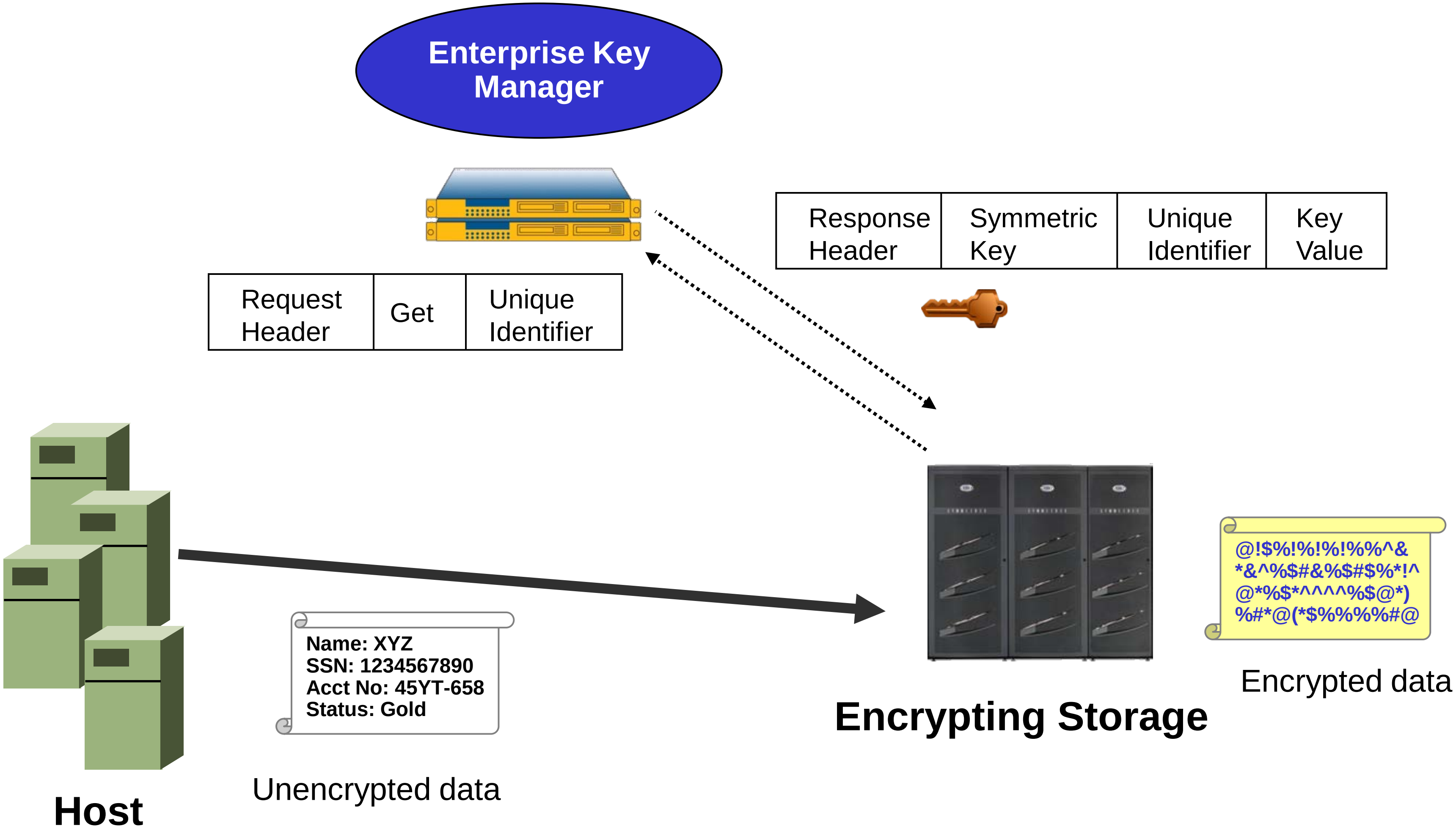
KMIP Objects, Operations and Attributes: Asymmetric Keys



KMIP Objects, Operations and Attributes: Digital Certificates



KMIP Request / Response Model



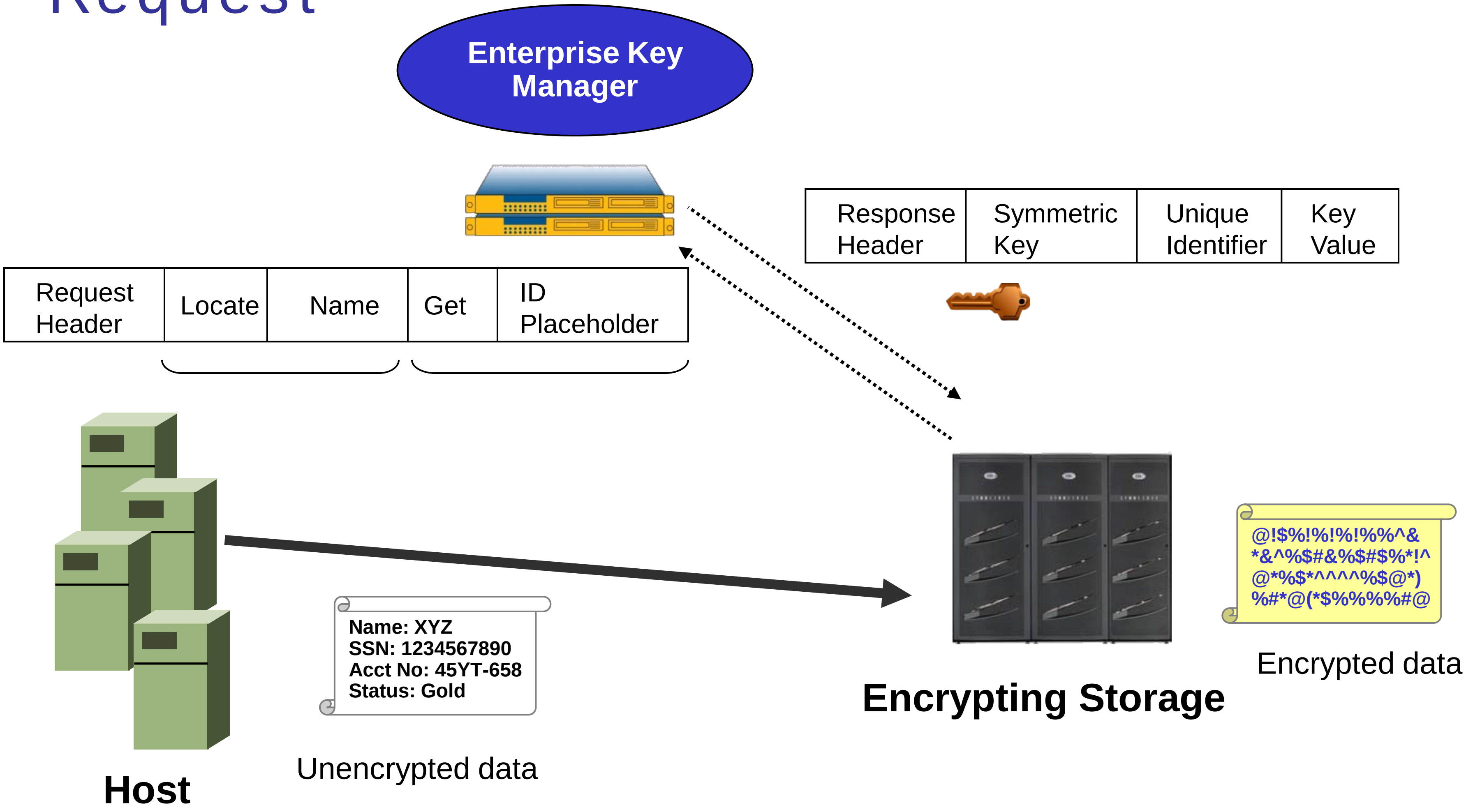
Response Header	Symmetric Key	Unique Identifier	Key Value

Request Header	Get	Unique Identifier

Name: XYZ
SSN: 1234567890
Acct No: 45YT-658
Status: Gold

@!$%!%!%!%%^&
&^%$#&%$#$%!^
@*%$*^^^^%$@*)
%#*@(*$%%%%#@

Supporting Multiple Operations per Request



Enterprise Key Manager

Response Header	Symmetric Key	Unique Identifier	Key Value

Request Header	Locate	Name	Get	ID Placeholder

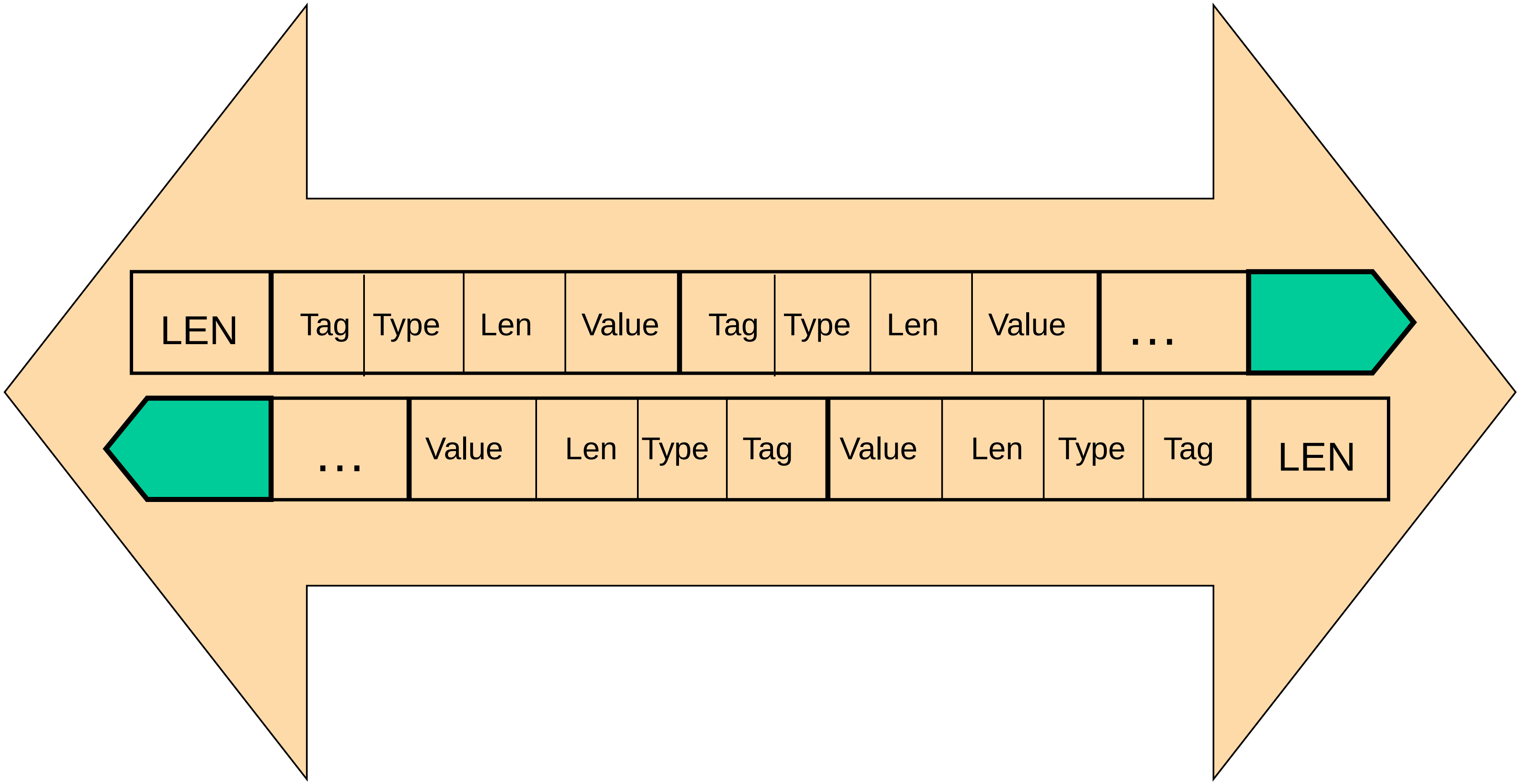
Name: XYZ
SSN: 1234567890
Acct No: 45YT-658
Status: Gold

Unencrypted data

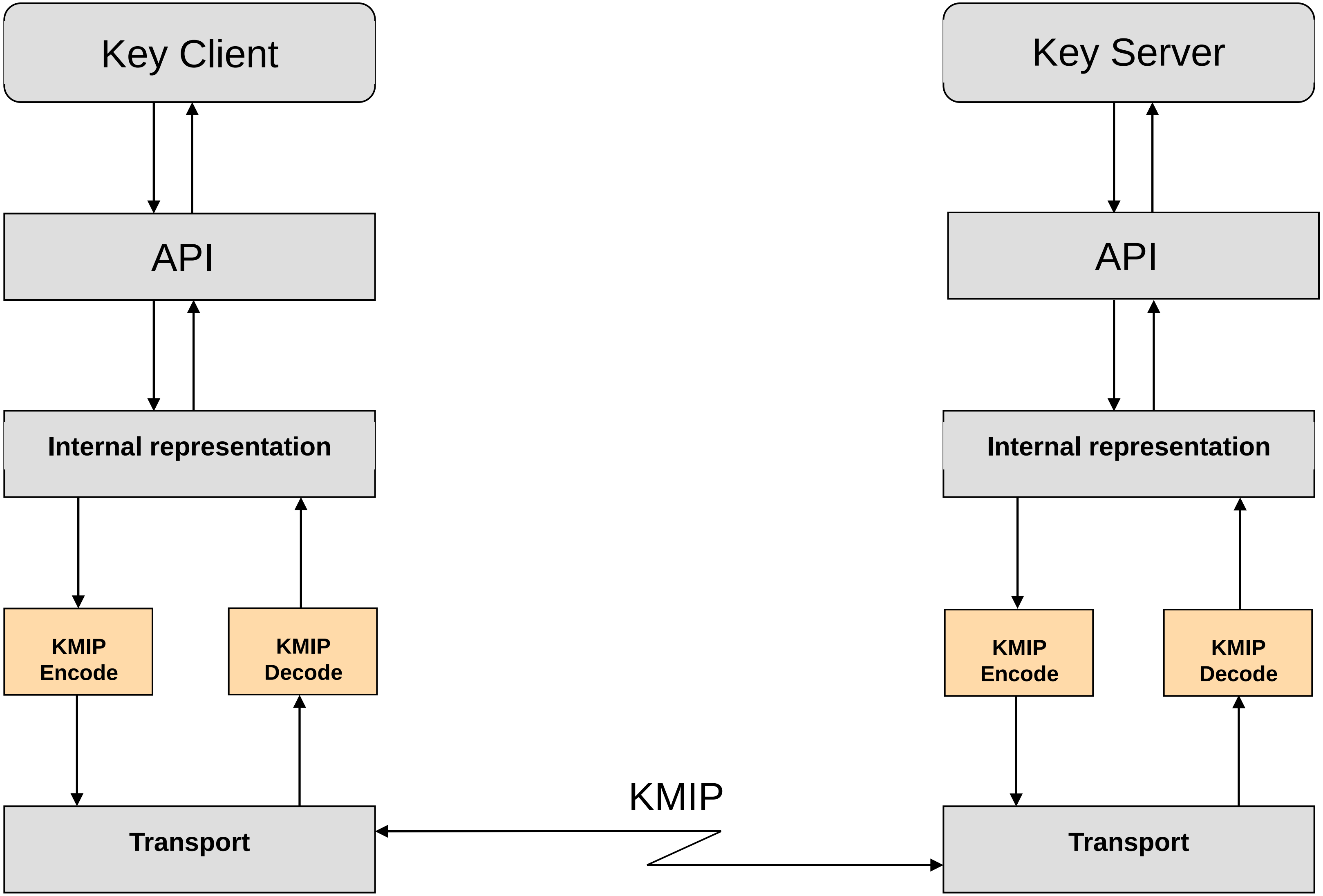
@!$%!%!%!%%^&
&^%$#&%$#$%!^
@*%$*^^^^%$@*)
%#*@(*$%%%%#@

Encrypted data

Messages in TTLV Format



Transport-Level Encoding



KMIP Message Overview

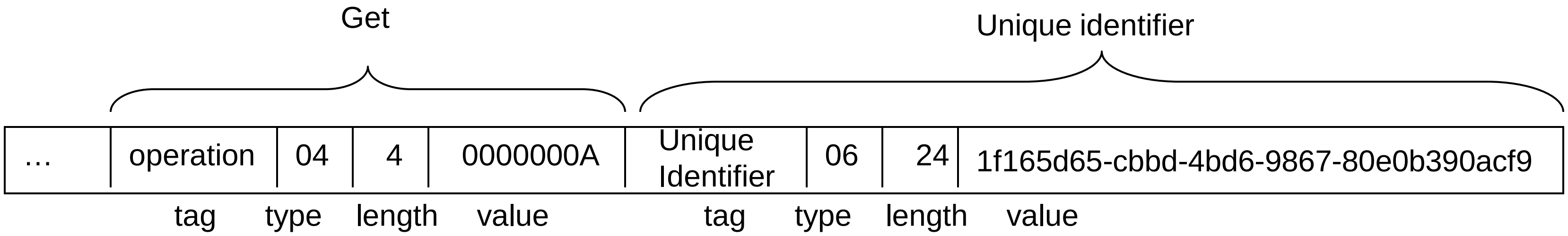
Message Encoding

- Example of TTLV encoding of the *Application Specific ID* Attribute
  - Attribute identified by its name “Application Specific ID”
  - Shows value at index 2

<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>Attribute</td><td>Structure</td><td>&lt;varies&gt;</td><td>
<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>Attribute Name</td><td>String</td><td>&lt;varies&gt;</td><td>“Application Specific ID”</td></tr>
<tr><td>Attribute Index</td><td>Integer</td><td>4</td><td>2</td></tr>
<tr><td>Attribute Value</td><td>Structure</td><td>&lt;varies&gt;</td><td>
<table>
<tr><th>Tag</th><th>Type</th><th>Length</th><th>Value</th></tr>
<tr><td>App. Name</td><td>String</td><td>&lt;varies&gt;</td><td>“ssl”</td></tr>
<tr><td>App. ID</td><td>String</td><td>&lt;varies&gt;</td><td>“www.example.com”</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

Message Encoding - 2

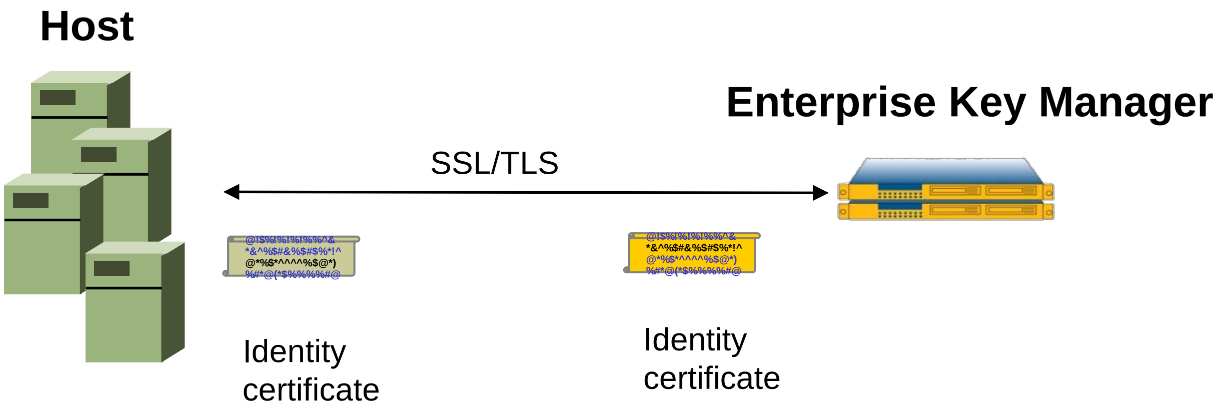
- In a TTLV-encoded message, Attributes are identified either by tag value or by their name (see previous slide), depending on the context:
  - When the operation lists the attribute name among the objects part of the request/response (such as Unique Identifier), its tag is used in the encoded message
  - When the operation does not list the attribute name explicitly, but instead includes Template-Attribute (such as in the Create operation) or Attribute (such as in Add Attribute) objects as part of the request/response, its name is used in the encoded message



	Get				Unique identifier			
…	operation	04	4	0000000A	Unique Identifier	06	24	1f165d65-cbbd-4bd6-9867-80e0b390acf9
	tag	type	length	value	tag	type	length	value

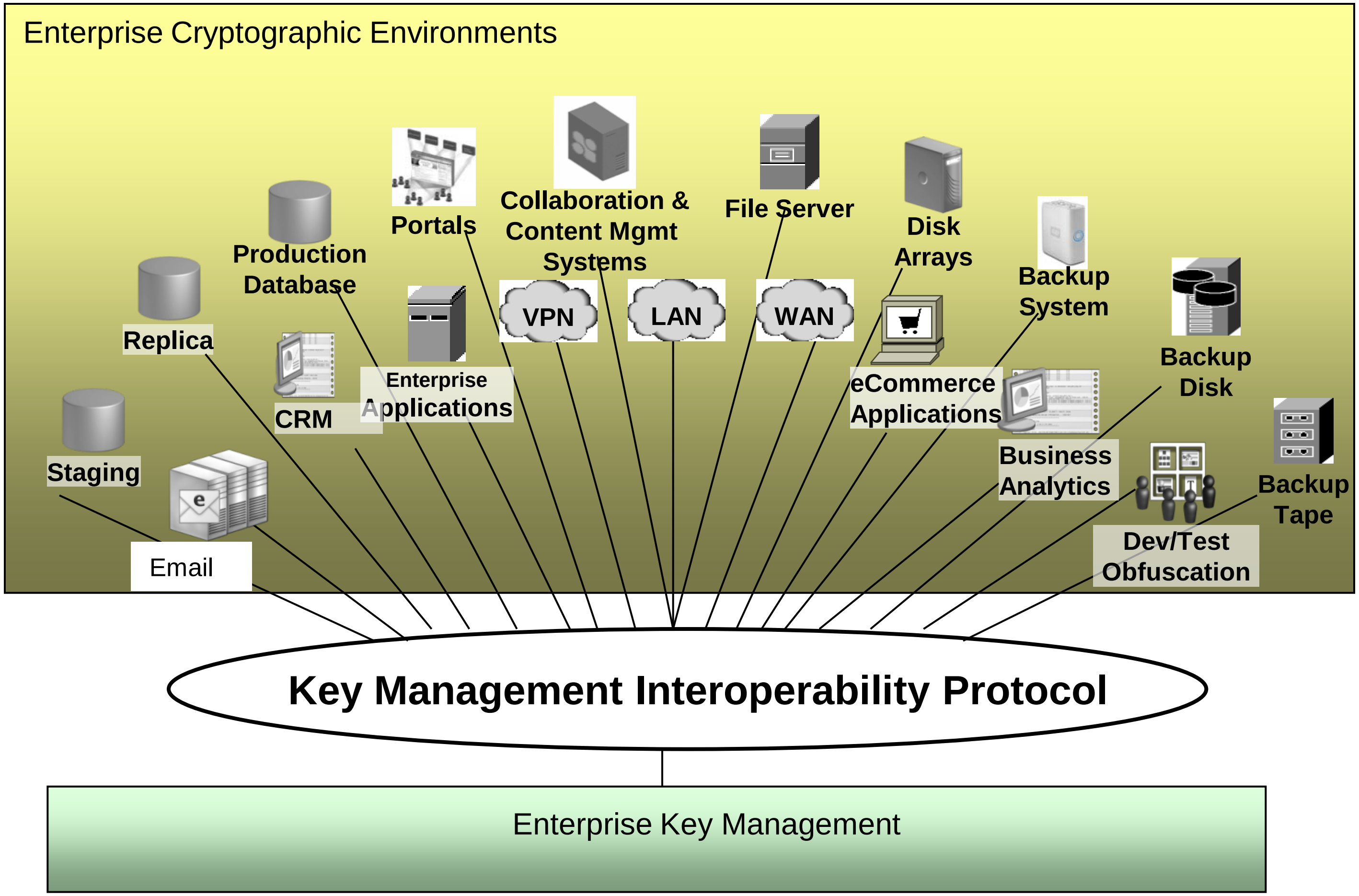
Authentication

- Authentication is external to the protocol
- All servers should support at least
  - SSL/TLS
  - https
- Authentication message field contains the Credential Base Object
  - Client or server certificate in the case of SSL/TLS or https



Conclusion

KMIP: enabling enterprise key management through standard protocol.



Questions?