Ensuring Confidentiality (and trust)

Encryption, Data Retrieval, and Key Management Technologies

Jerry Smith, US Department of Defense

Anthony Rutkowski, Yaana Technologies

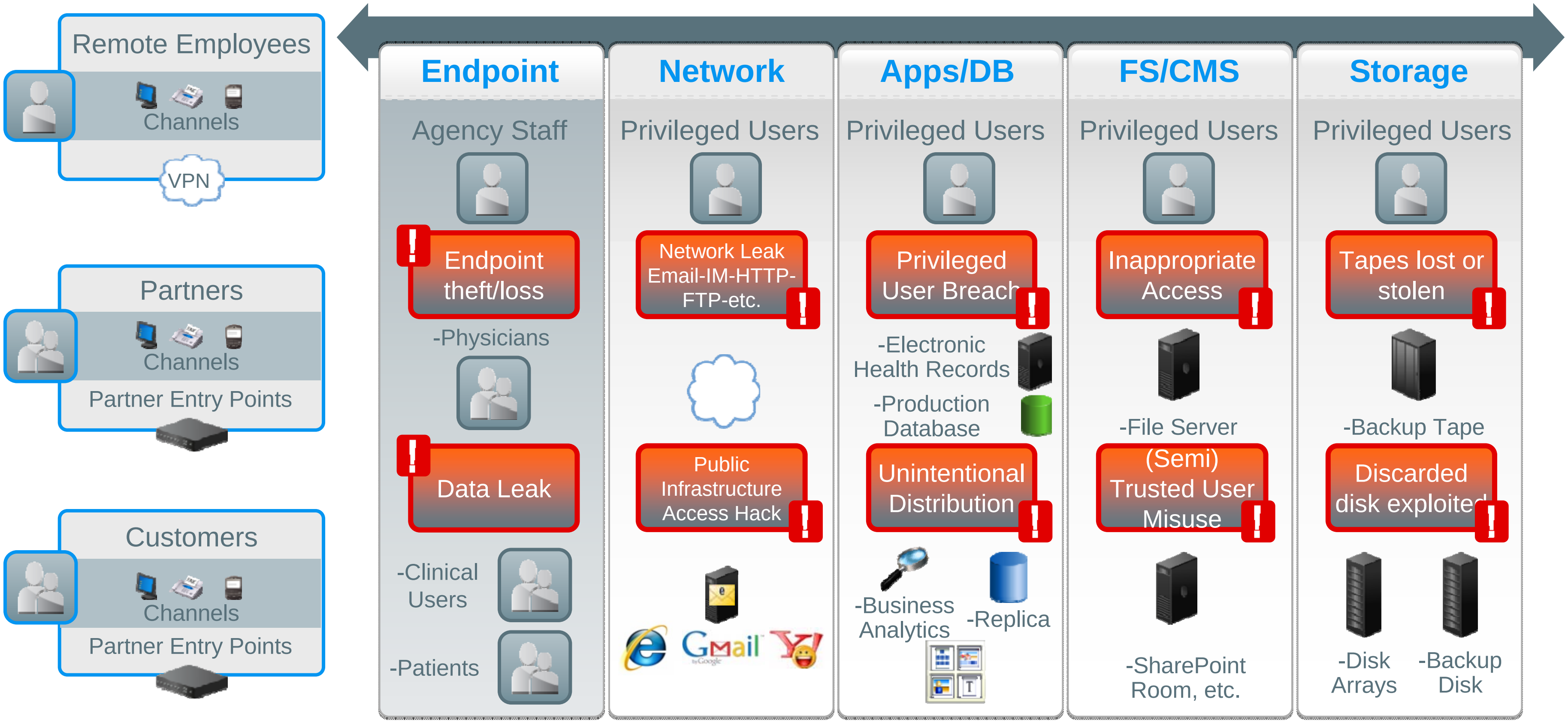
Bob Griffin, RSA, the Security Division of EMC

Ensuring confidentiality and trust …

… is not easy

- Information growth
- Mobility, virtualization & cloud

- Evolving threat landscape
- Collaboration / Exchange



Remote Employees
Channels
VPN

Partners
Channels
Partner Entry Points

Customers
Channels
Partner Entry Points

Endpoint
Agency Staff
Endpoint theft/loss
-Physicians
Data Leak
-Clinical Users
-Patients

Network
Privileged Users
Network Leak Email-IM-HTTP-FTP-etc.
Public Infrastructure Access Hack

Apps/DB
Privileged Users
Privileged User Breach
-Electronic Health Records
-Production Database
Unintentional Distribution
-Business Analytics
-Replica

FS/CMS
Privileged Users
Inappropriate Access
-File Server
(Semi) Trusted User Misuse
-SharePoint Room, etc.

Storage
Privileged Users
Tapes lost or stolen
-Backup Tape
Discarded disk exploited
-Disk Arrays
-Backup Disk

Ensuring Confidentiality (and trust):

the Extended Validation Certificate Platform

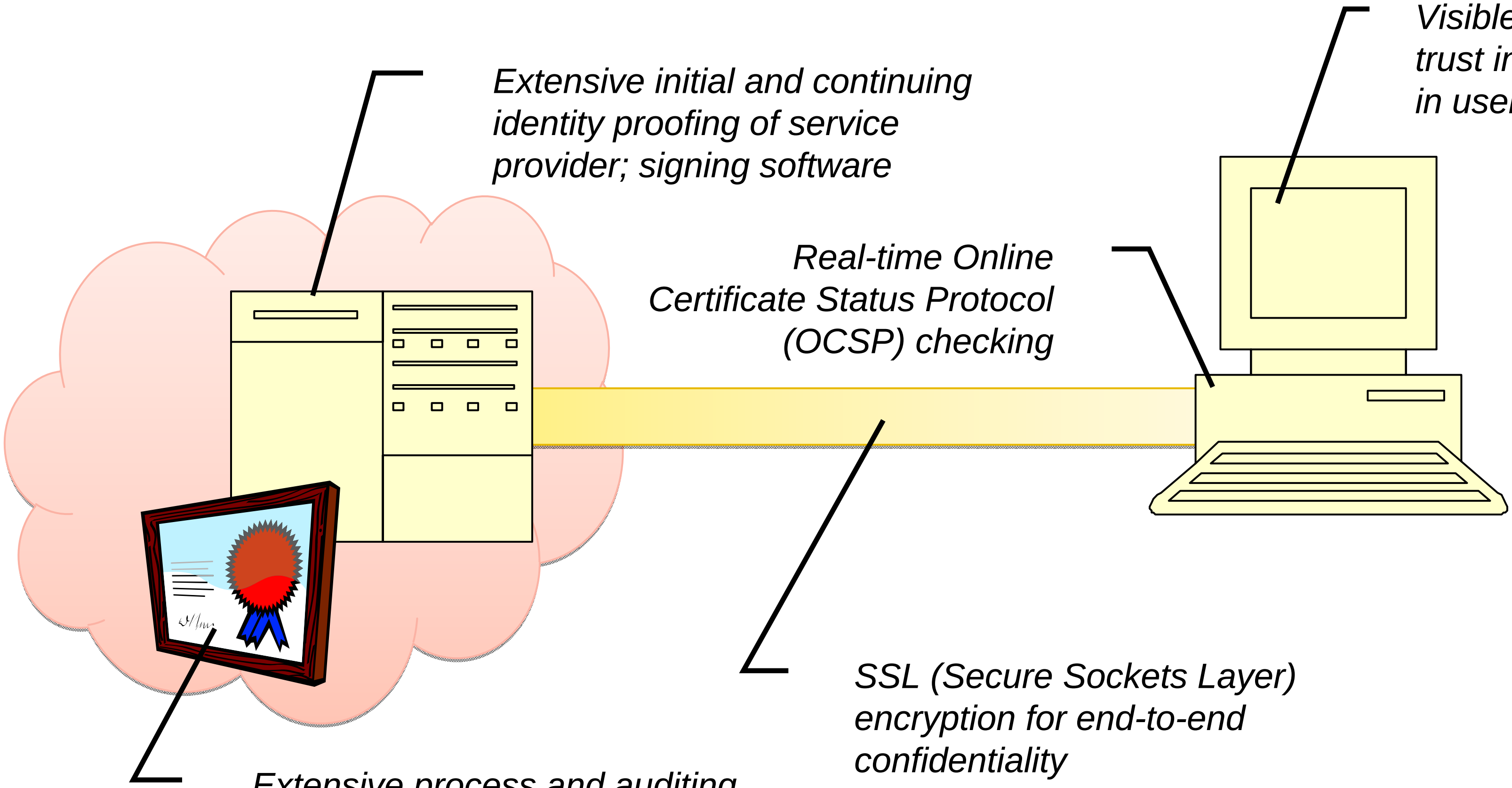
Tony Rutkowski

SVP for Regulatory Affairs and Standards, Yaana Technologies
ITU-T Rapporteur for Cybersecurity
Editor, Rec. ITU-T X.evcert
Liaison, CA/Browser Forum

EVcerts: critical for IdM and cybersecurity

- Trust in network sites and providers is critical to achieving effective Identity Management and cybersecurity
  - adverse effects include harm to users, other providers, and the infrastructure; loss of assurance
- The Extended Validation Certificate platform bundles together a proven set of technologies and practices to
  - significantly enhance trust assurance in the site/provider
  - create an encrypted path with the site
  - sign software

Some of what the EVcert platform provides



Visible EVcert trust indication in user browser

Extensive initial and continuing identity proofing of service provider; signing software

Real-time Online Certificate Status Protocol (OCSP) checking

SSL (Secure Sockets Layer) encryption for end-to-end confidentiality

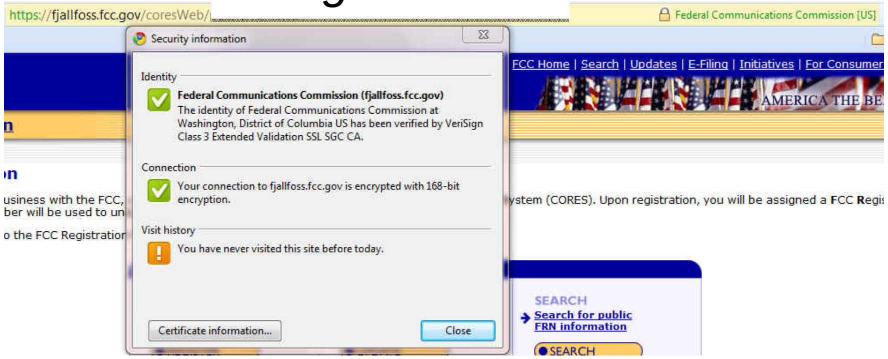
Extensive process and auditing requirements for issuing EVcert authorities

Additional value proposition

- CA/Browser Forum: developed and initially implemented by the most prominent software and digital certificate vendors worldwide over the past several years
- The platform has been included as a core capability in security standards by ETSI, Liberty Alliance, and ISO
- The platform is completely “open” and promotes a competitive environment
- ITU-T is importing and promulgating the platform for adoption in early 2011 as the X.evcert Framework to enhance global ubiquity and further its development
- Version 1.3 includes features to enhance use for cloud computing

How browsers display EVcert information

Google Chrome



https://fjallfoss.fcc.gov/coresWeb/ — Federal Communications Commission [US]

Security information

Identity

Federal Communications Commission (fjallfoss.fcc.gov)
The identity of Federal Communications Commission at Washington, District of Columbia US has been verified by VeriSign Class 3 Extended Validation SSL SGC CA.

Connection

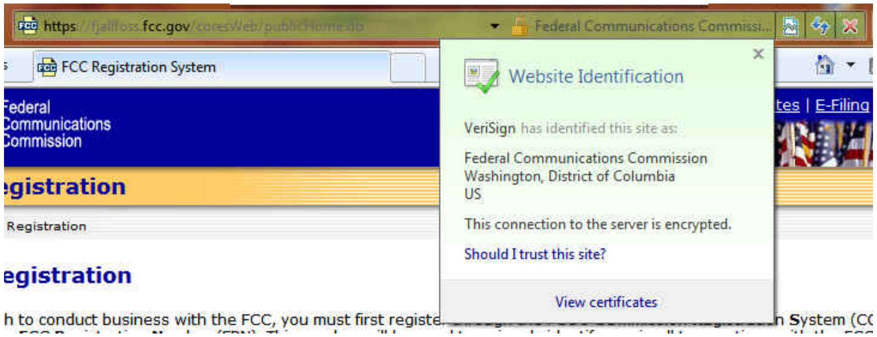
Your connection to fjallfoss.fcc.gov is encrypted with 168-bit encryption.

Visit history

You have never visited this site before today.

Certificate information...
Close
FCC Home | Search | Updates | E-Filing | Initiatives | For Consumer
SEARCH
Search for public FRN information

Microsoft Explorer 8.0



https://fjallfoss.fcc.gov/coresWeb/publicHome.do — Federal Communications Commissi...

FCC Registration System

Website Identification

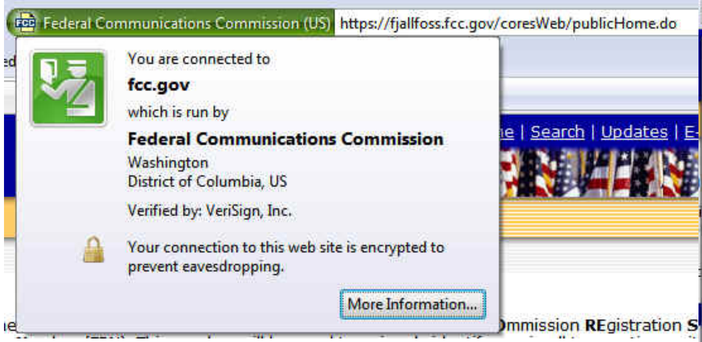
VeriSign has identified this site as:

Federal Communications Commission
Washington, District of Columbia
US

This connection to the server is encrypted.

Should I trust this site?

Mozilla Firefox 3.1 pre



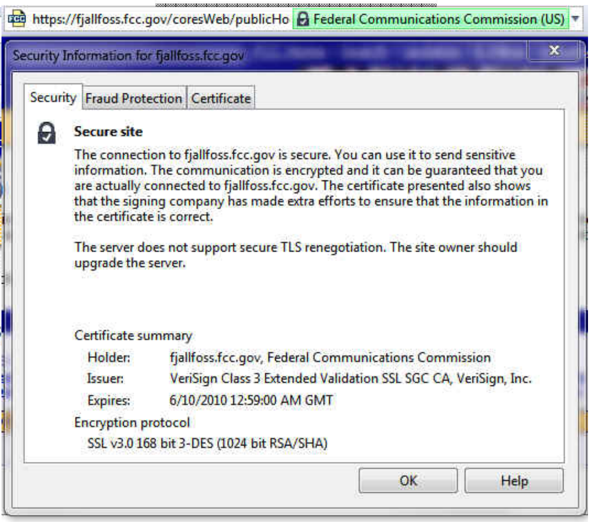
Federal Communications Commission (US) https://fjallfoss.fcc.gov/coresWeb/publicHome.do

You are connected to
fcc.gov
which is run by
Federal Communications Commission
Washington
District of Columbia, US

Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

Opera 10.51



https://fjallfoss.fcc.gov/coresWeb/publicHo — Federal Communications Commission (US)

Security Information for fjallfoss.fcc.gov

Secure site

The connection to fjallfoss.fcc.gov is secure. You can use it to send sensitive information. The communication is encrypted and it can be guaranteed that you are actually connected to fjallfoss.fcc.gov. The certificate presented also shows that the signing company has made extra efforts to ensure that the information in the certificate is correct.

The server does not support secure TLS renegotiation. The site owner should upgrade the server.

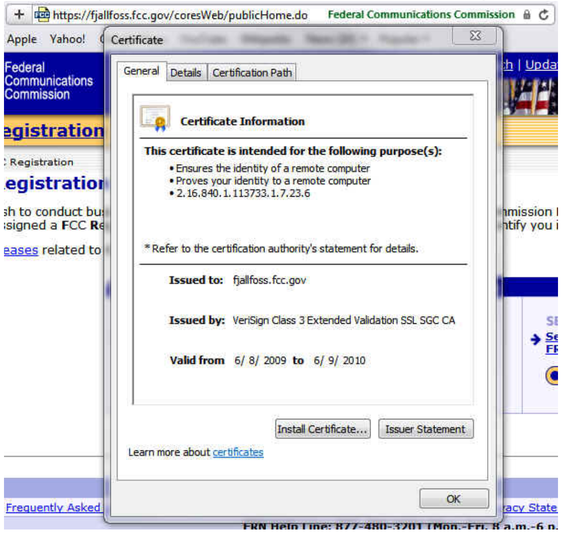
Certificate summary

Holder: fjallfoss.fcc.gov, Federal Communications Commission
Issuer: VeriSign Class 3 Extended Validation SSL SGC CA, VeriSign, Inc.
Expires: 6/10/2010 12:59:00 AM GMT

Encryption protocol

SSL v3.0 168 bit 3-DES (1024 bit RSA/SHA)

Apple Safari 4.0.5



https://fjallfoss.fcc.gov/coresWeb/publicHome.do — Federal Communications Commission

Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.113733.1.7.23.6

* Refer to the certification authority's statement for details.

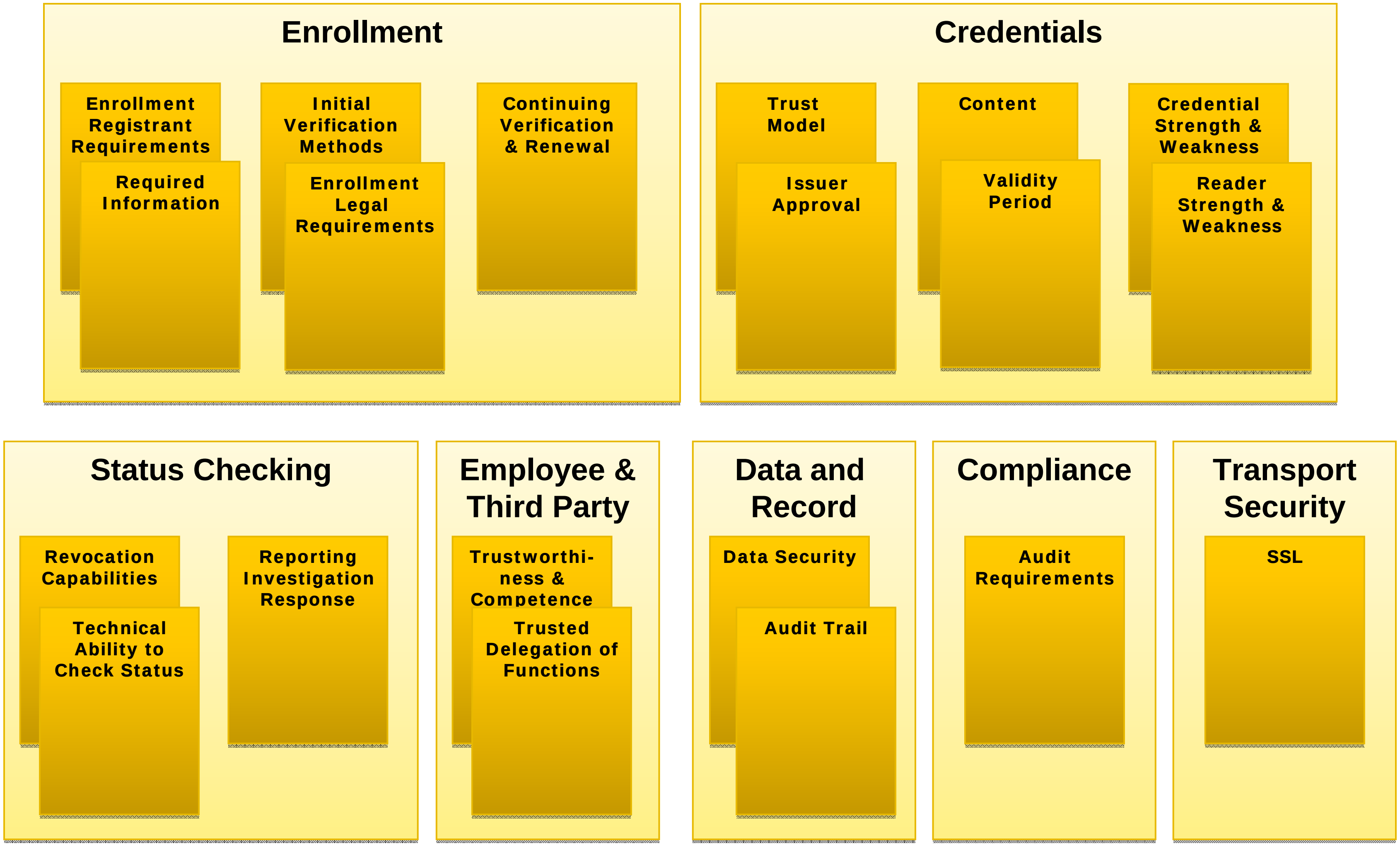
Issued to: fjallfoss.fcc.gov

Issued by: VeriSign Class 3 Extended Validation SSL SGC CA

Valid from 6/ 8/ 2009 **to** 6/ 9/ 2010

Learn more about certificates

Comprehensive specification and continuing examination/evolution



Enrollment

- Enrollment Registrant Requirements
- Required Information
- Initial Verification Methods
- Enrollment Legal Requirements
- Continuing Verification & Renewal

Credentials

- Trust Model
- Issuer Approval
- Content
- Validity Period
- Credential Strength & Weakness
- Reader Strength & Weakness

Status Checking

- Revocation Capabilities
- Technical Ability to Check Status
- Reporting Investigation Response

Employee & Third Party

- Trustworthiness & Competence
- Trusted Delegation of Functions

Data and Record

- Data Security
- Audit Trail

Compliance

- Audit Requirements

Transport Security

- SSL

Extensible roadmap

- New kinds of organizations
- New applications
- Expanded geographical coverage and assurance schemas
- Expanded Cloud IdM use
- Enhanced user visual indicators

Ensuring Confidentiality (and trust):

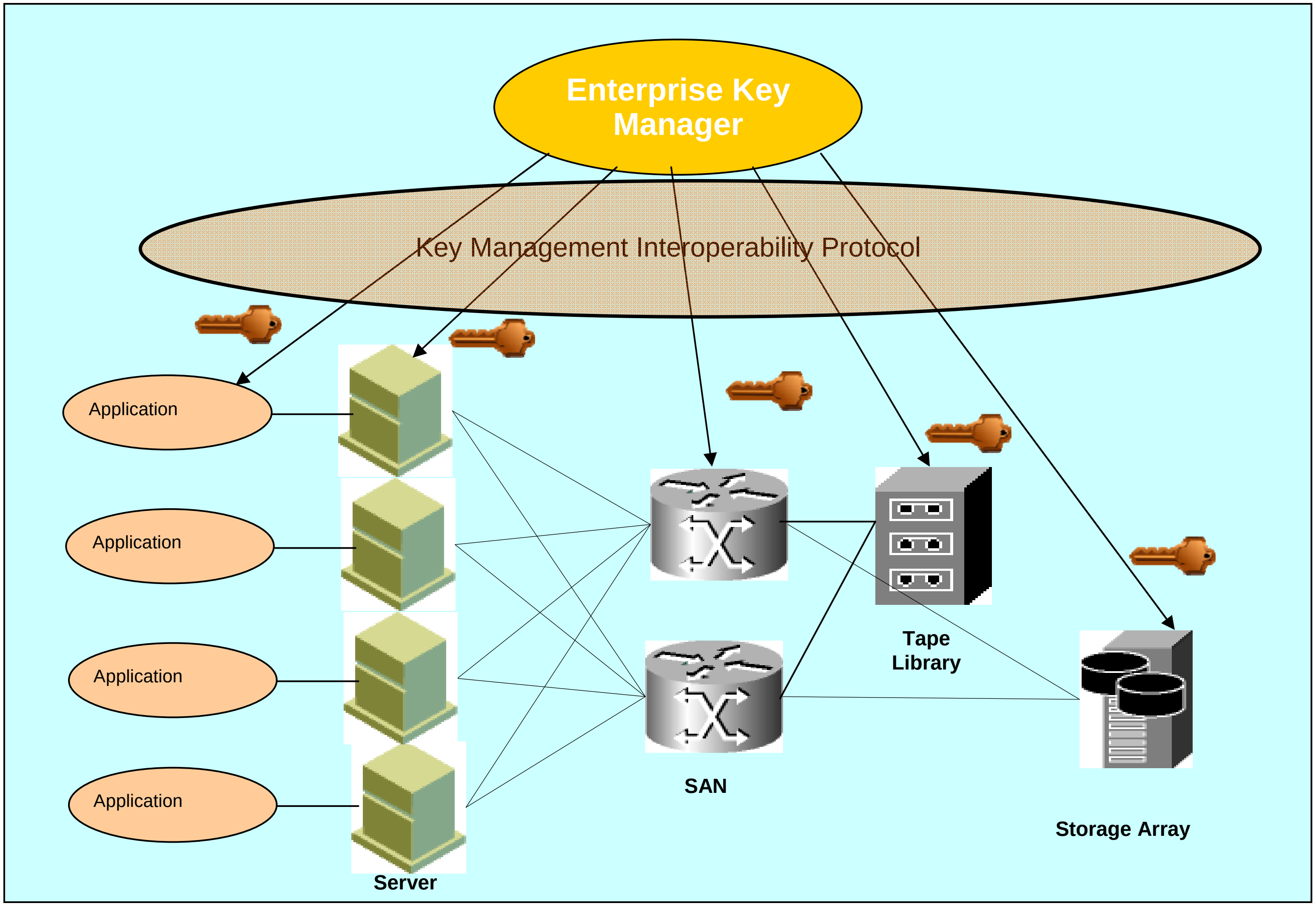
Extending Enterprise Key Management to Infrastructure Entity Authentication

Bob Griffin

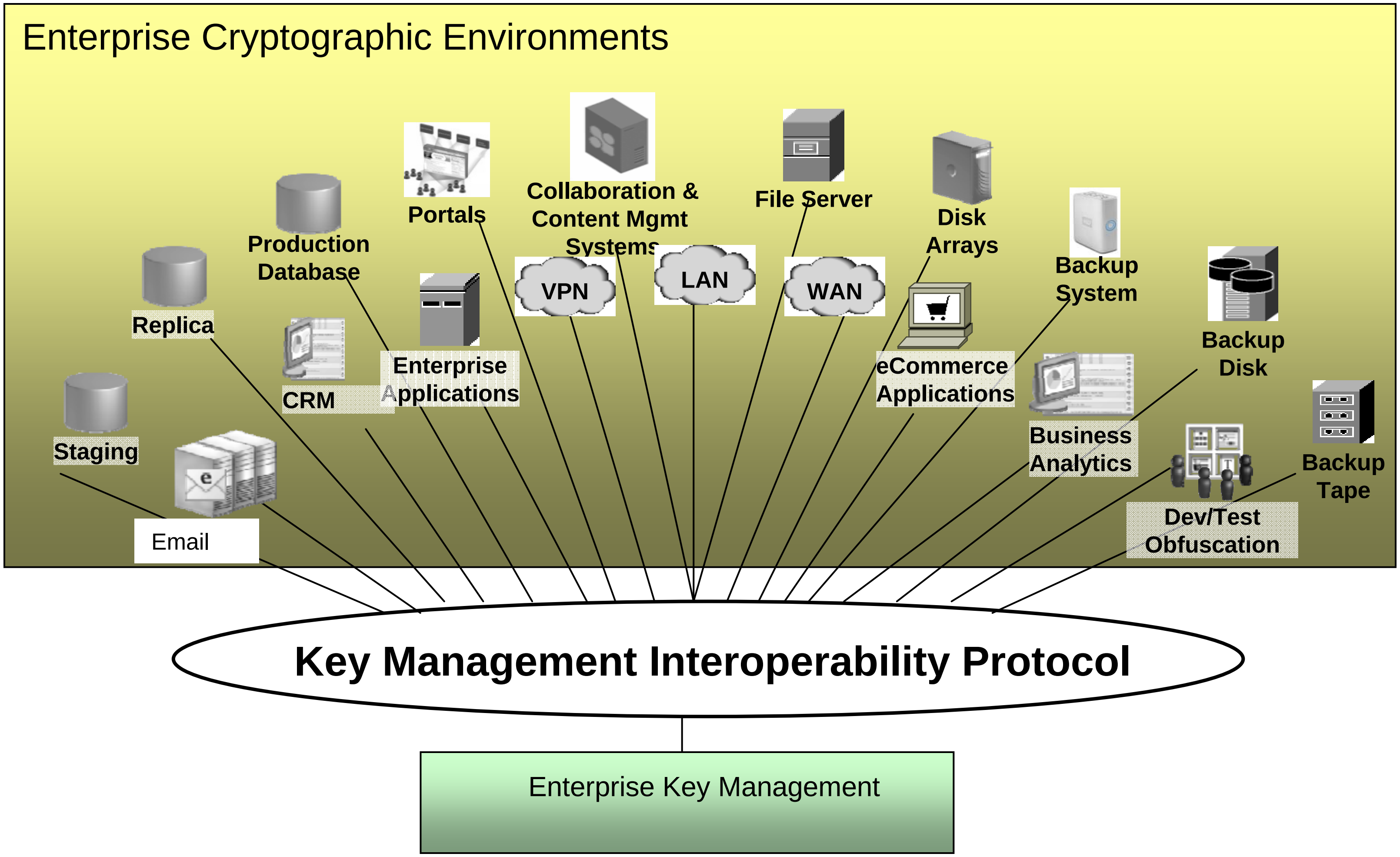
Technical Director, RSA, the Security Division of EMC

Co-chair, OASIS Key Management Interoperability Protocol TC

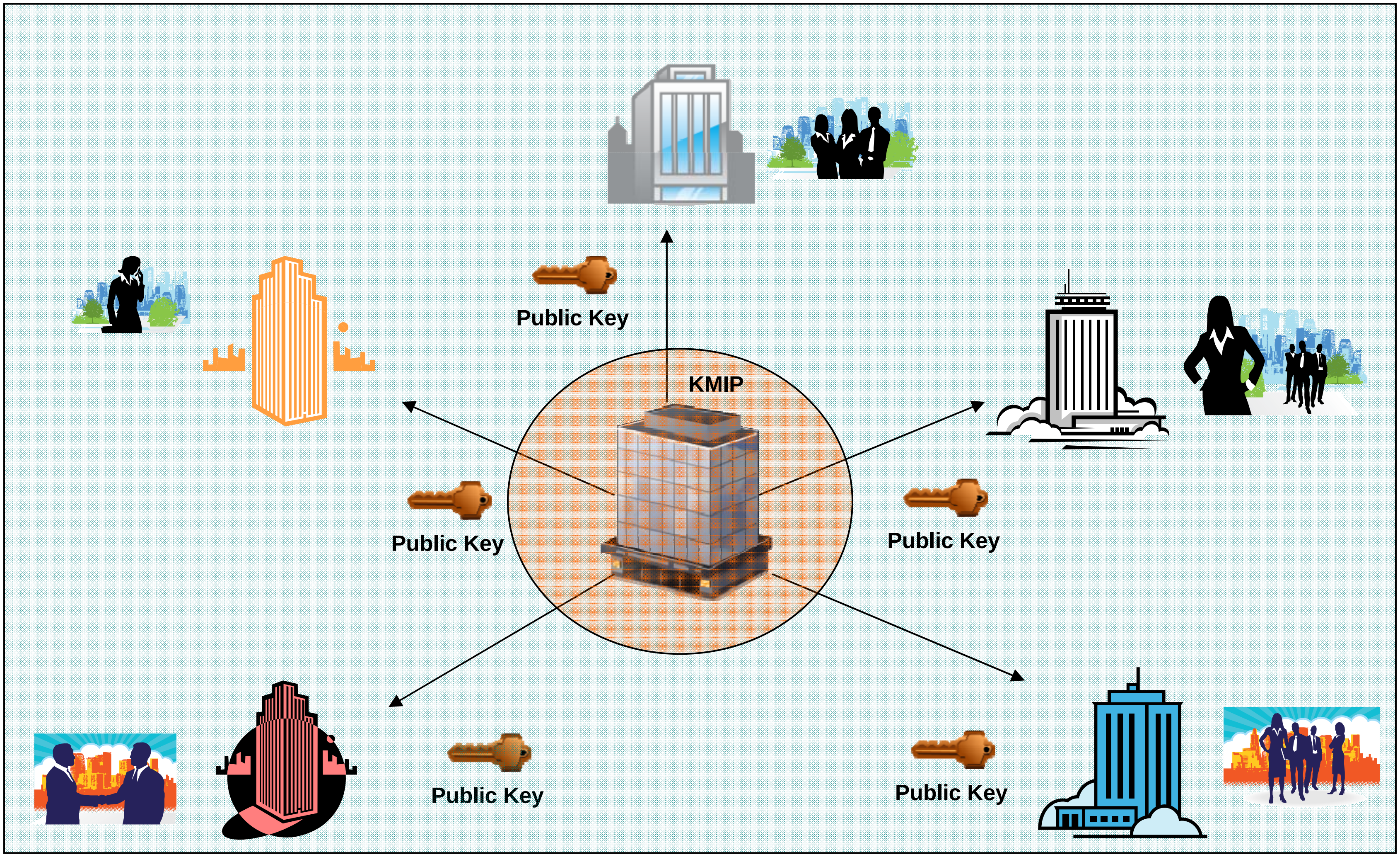
Data Encryption using Symmetric Keys



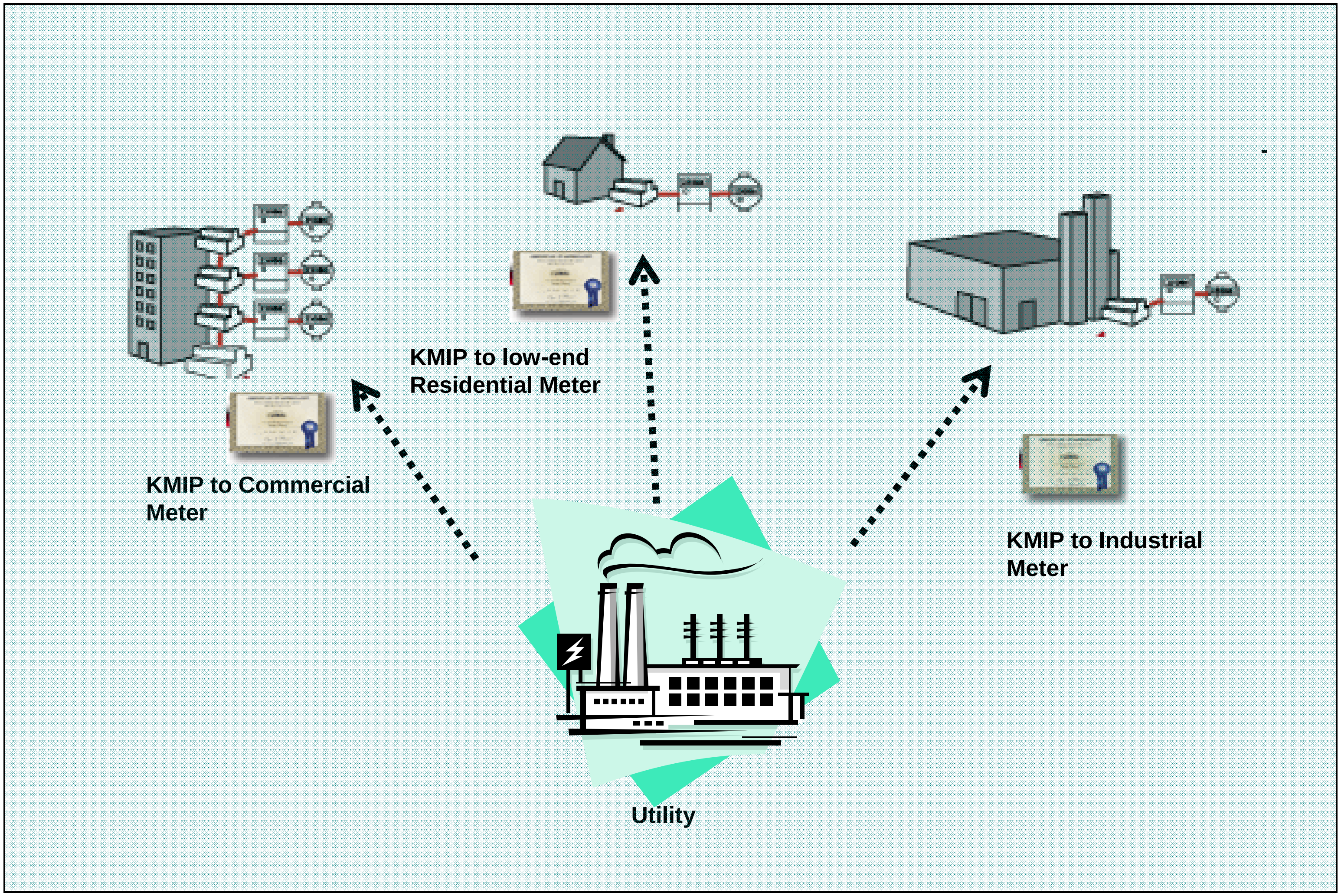
KMIP: Single Protocol Supporting Enterprise Cryptographic Environments



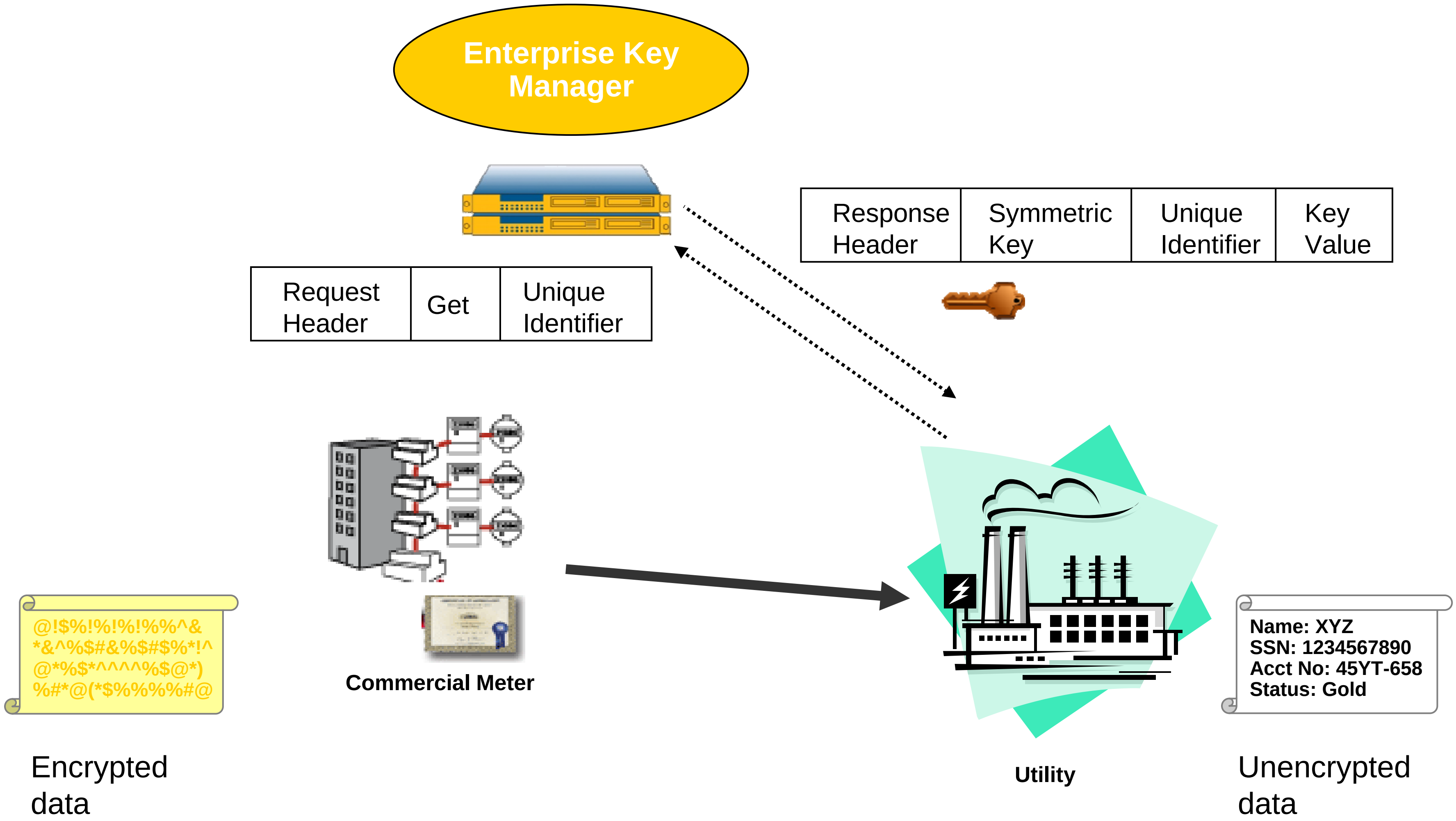
User Identity with Asymmetric Keys



Infrastructure Entity Identification



KMIP Request / Response Model



Enterprise Key Manager

Response Header	Symmetric Key	Unique Identifier	Key Value

Request Header	Get	Unique Identifier

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

Encrypted data

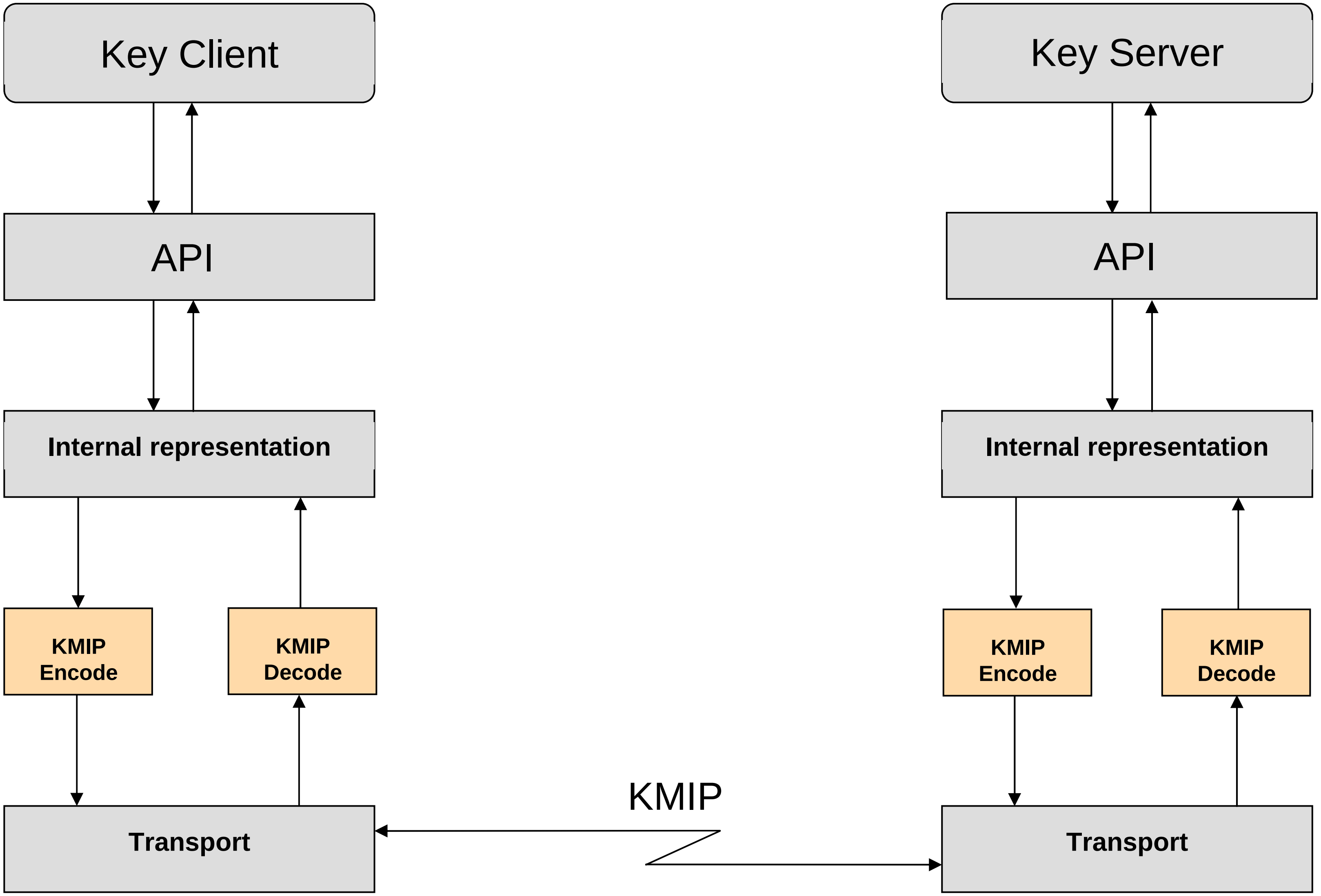
Commercial Meter

Utility

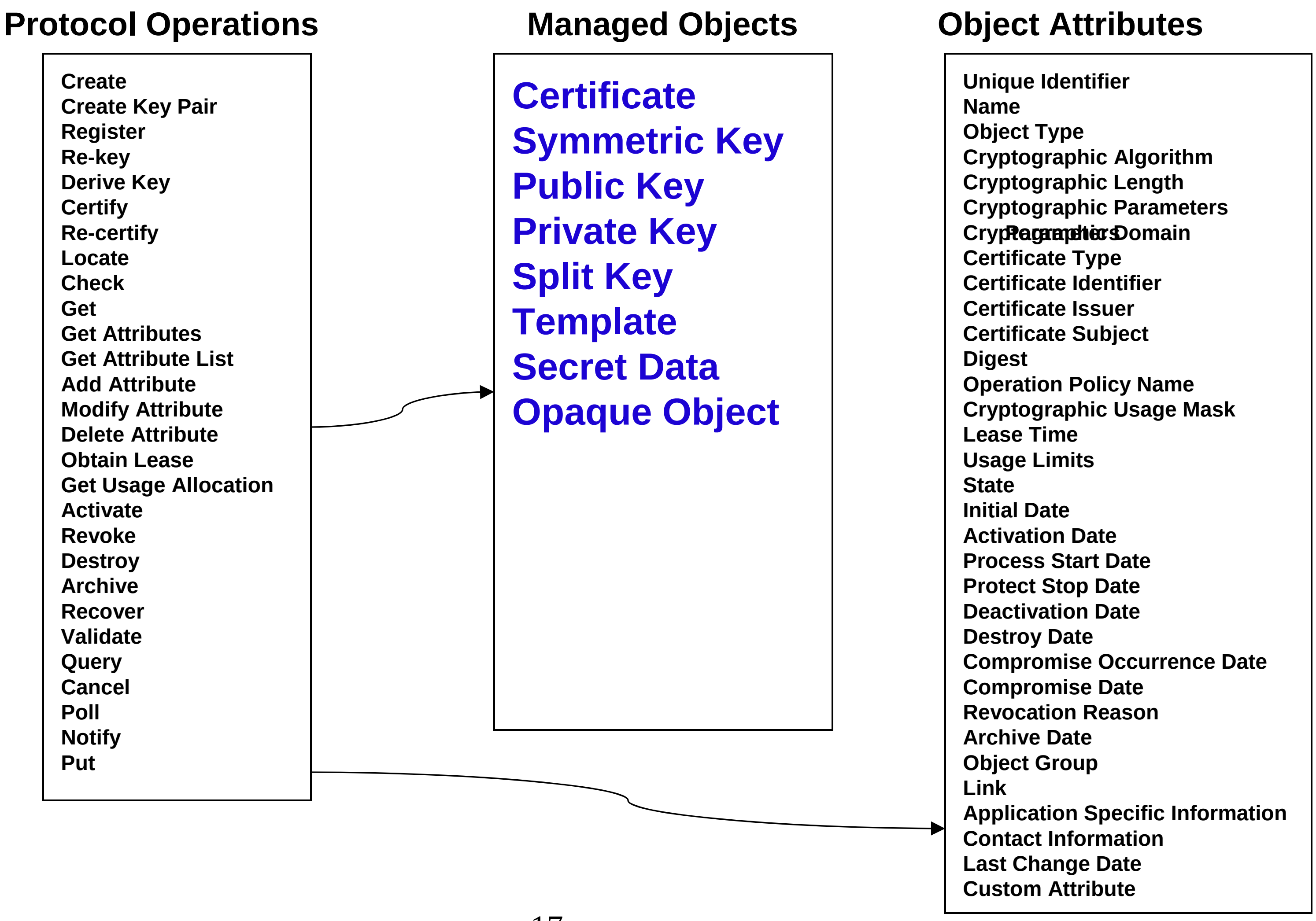
Name: XYZ
SSN: 1234567890
Acct No: 45YT-658
Status: Gold

Unencrypted data

Transport-Level Encoding



Objects, Operations and Attributes



Protocol Operations

- Create
- Create Key Pair
- Register
- Re-key
- Derive Key
- Certify
- Re-certify
- Locate
- Check
- Get
- Get Attributes
- Get Attribute List
- Add Attribute
- Modify Attribute
- Delete Attribute
- Obtain Lease
- Get Usage Allocation
- Activate
- Revoke
- Destroy
- Archive
- Recover
- Validate
- Query
- Cancel
- Poll
- Notify
- Put

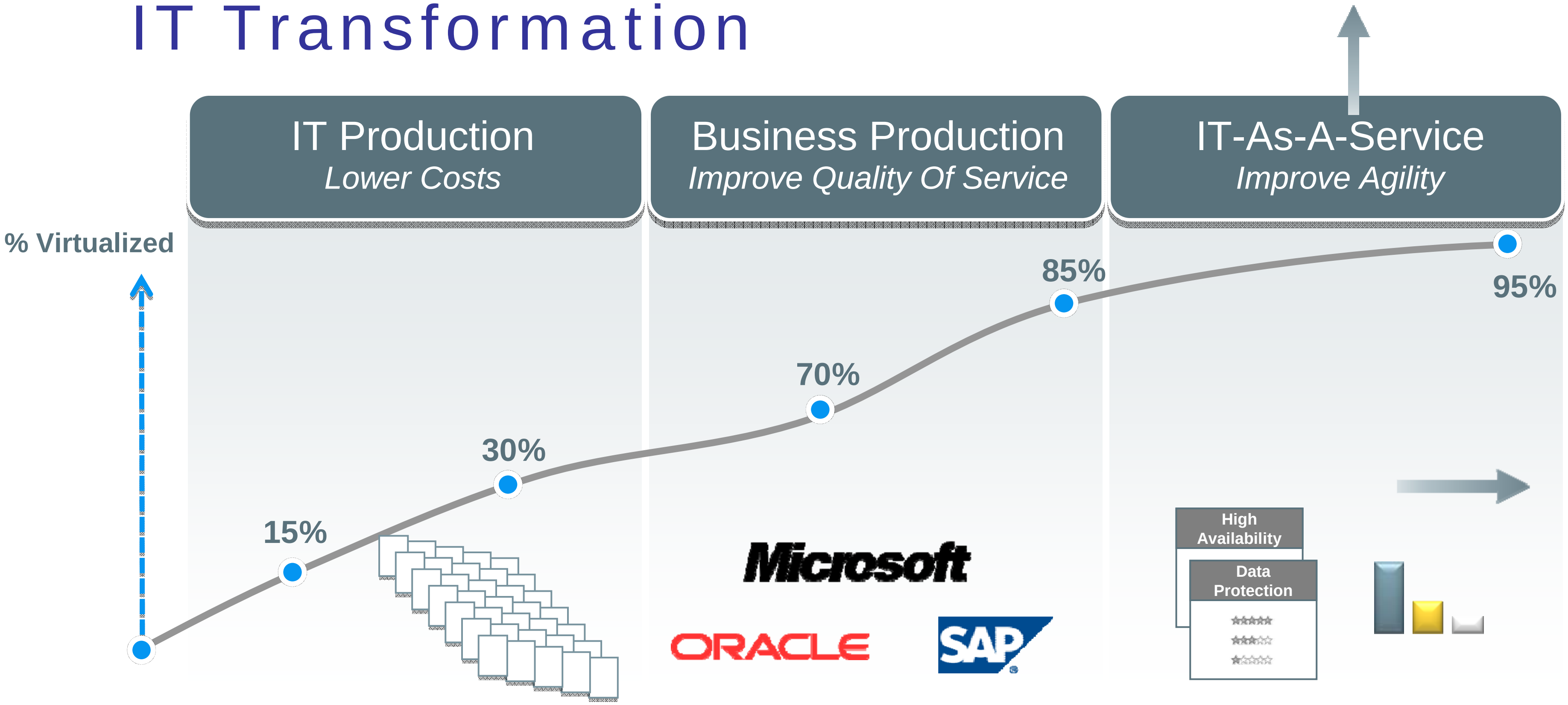
Managed Objects

- Certificate
- Symmetric Key
- Public Key
- Private Key
- Split Key
- Template
- Secret Data
- Opaque Object

Object Attributes

- Unique Identifier
- Name
- Object Type
- Cryptographic Algorithm
- Cryptographic Length
- Cryptographic Parameters
- Cryptographic Domain Parameters
- Certificate Type
- Certificate Identifier
- Certificate Issuer
- Certificate Subject
- Digest
- Operation Policy Name
- Cryptographic Usage Mask
- Lease Time
- Usage Limits
- State
- Initial Date
- Activation Date
- Process Start Date
- Protect Stop Date
- Deactivation Date
- Destroy Date
- Compromise Occurrence Date
- Compromise Date
- Revocation Reason
- Archive Date
- Object Group
- Link
- Application Specific Information
- Contact Information
- Last Change Date
- Custom Attribute

IT Transformation

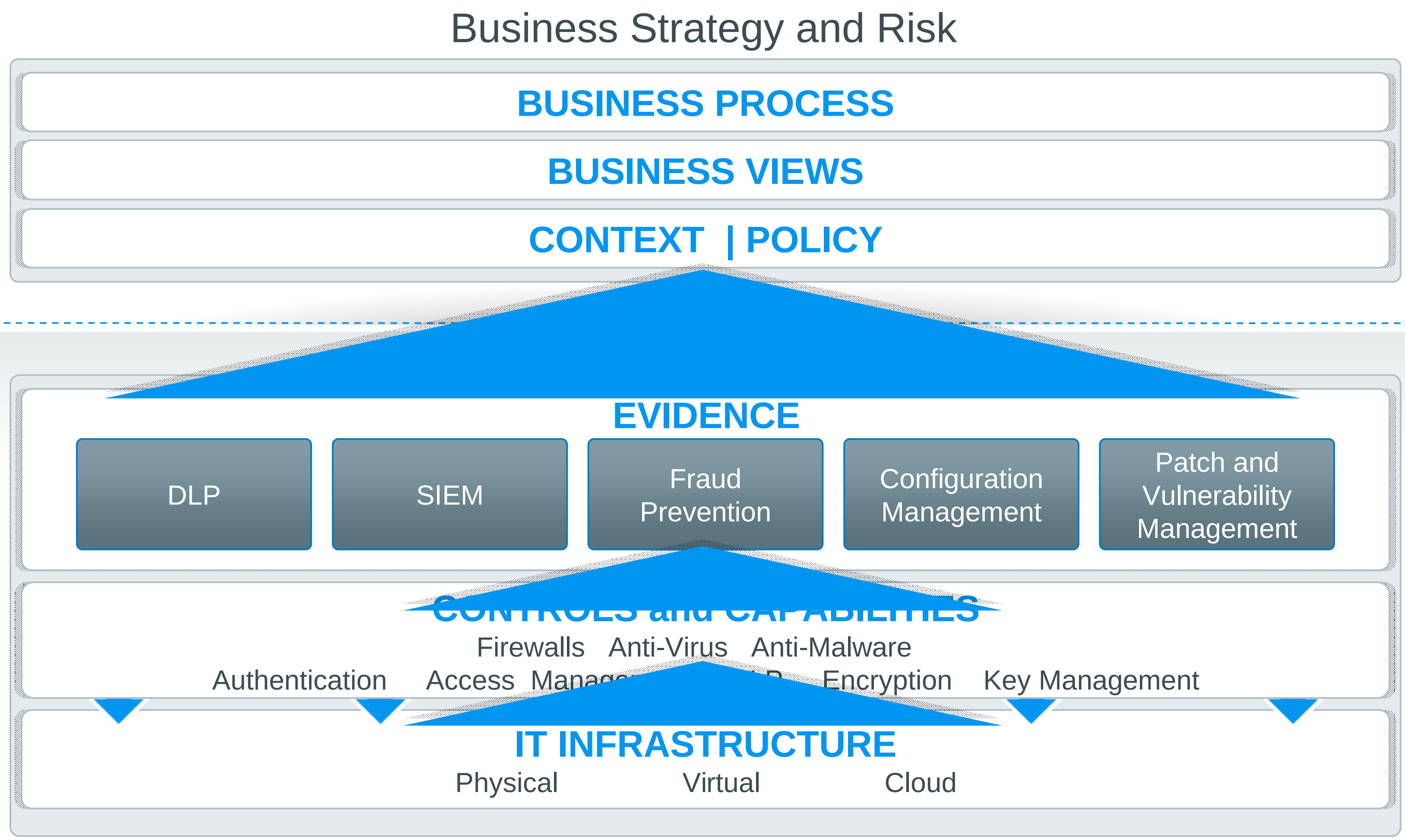


☑ **Secure multi-tenancy, verifiable chain fo trust.**

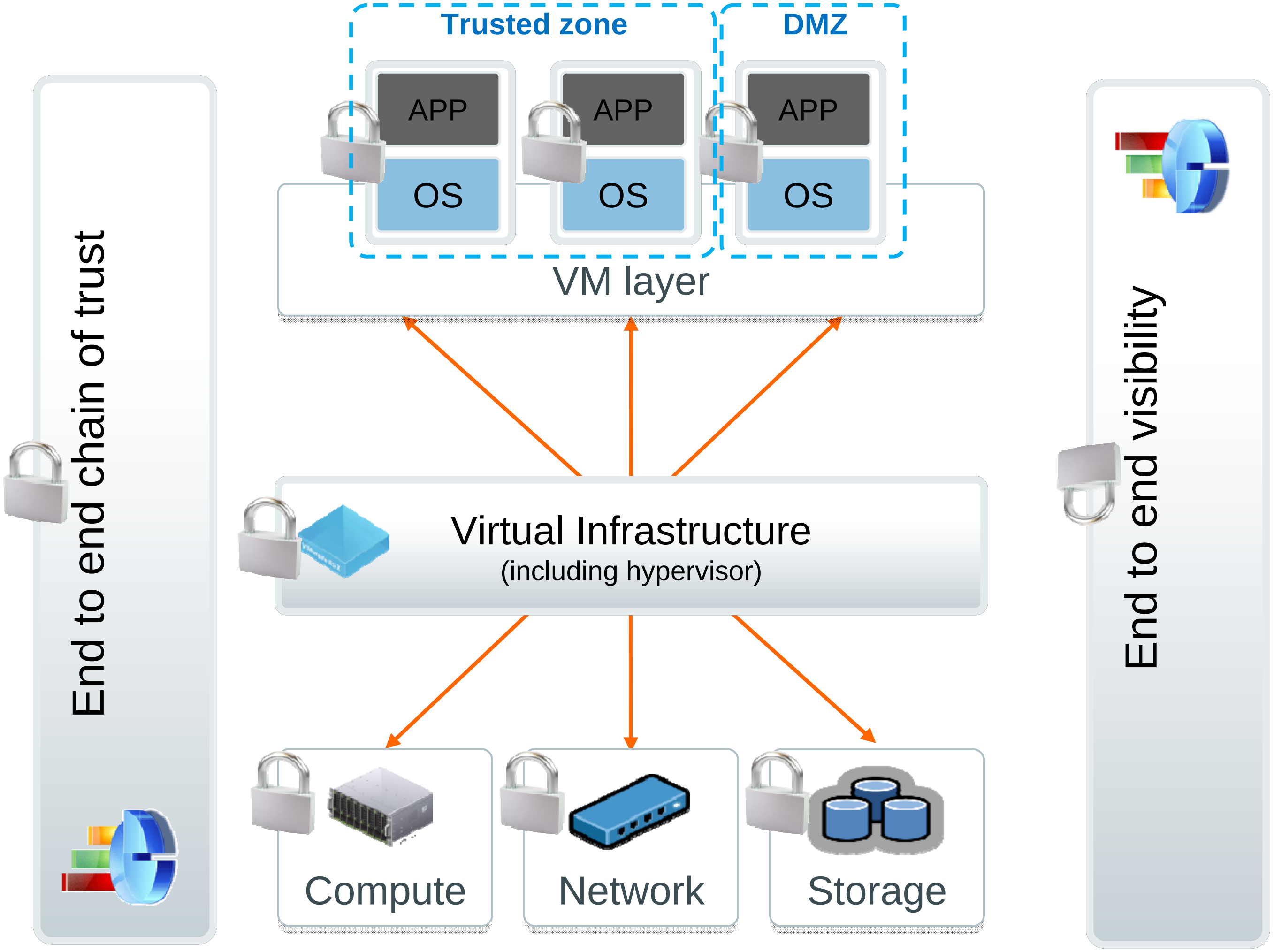
☑ **Information-centric security, risk-driven policies, IT and security operations in alignment, information compliance**

☑ **Visibility into virtualization infrastructure, privileged user monitoring, access management, network security, infrastructure compliance**

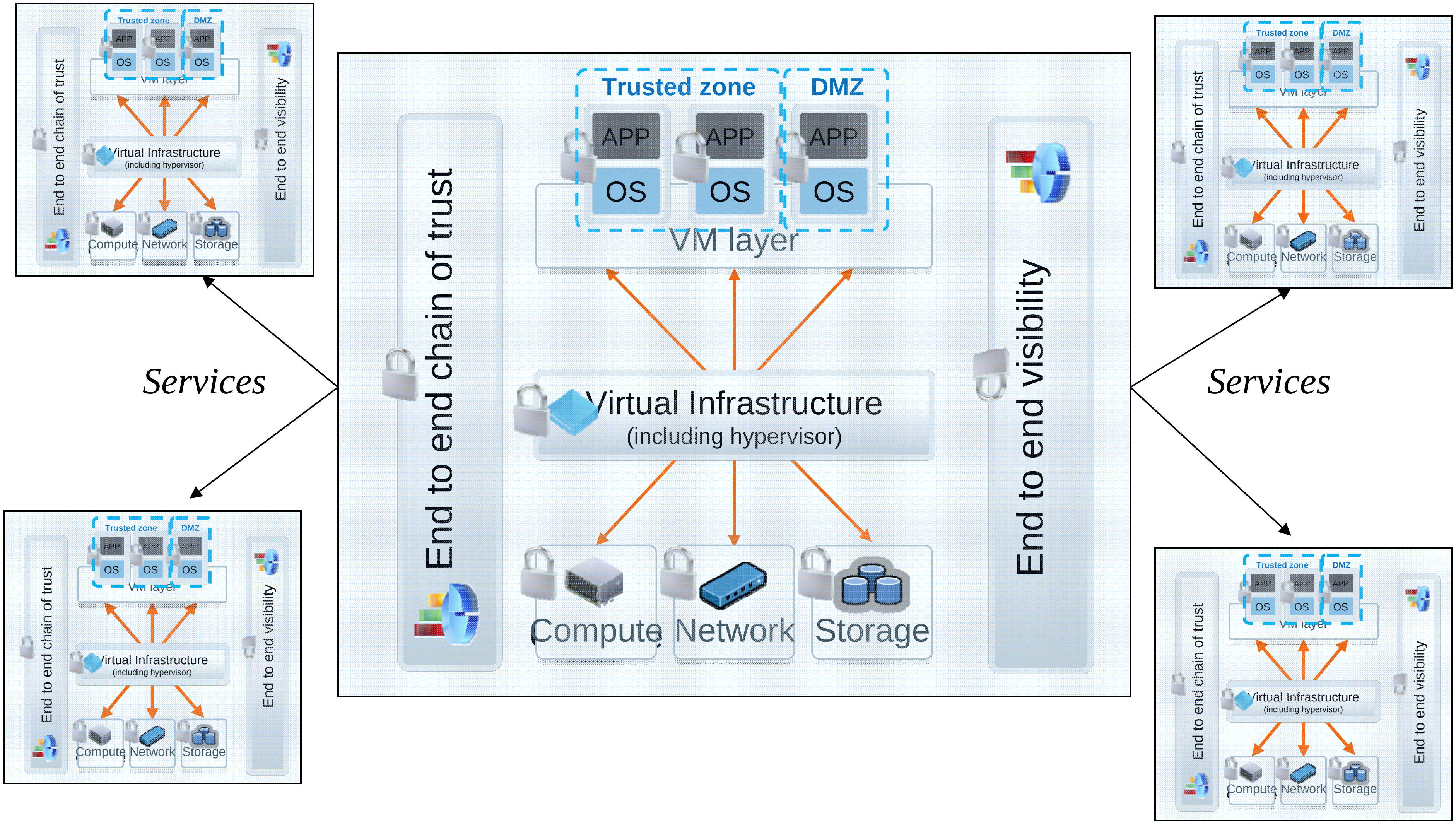
Security as a System



The Need to Extend Enterprise Key Management



Establishing the Web of Trust



Services

Services