

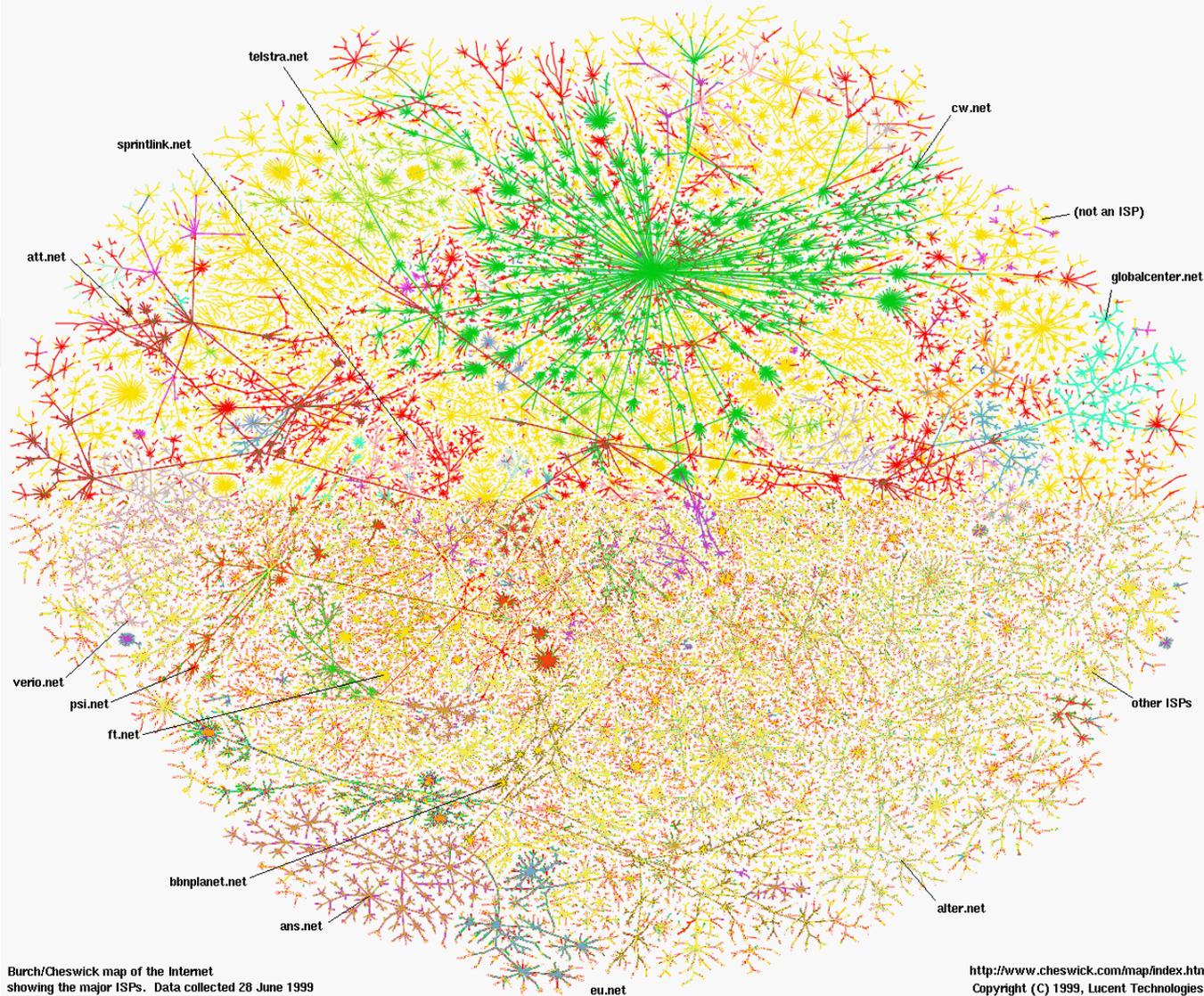


# A Consolidated Security Mechanism for the Entire Utility Enterprise

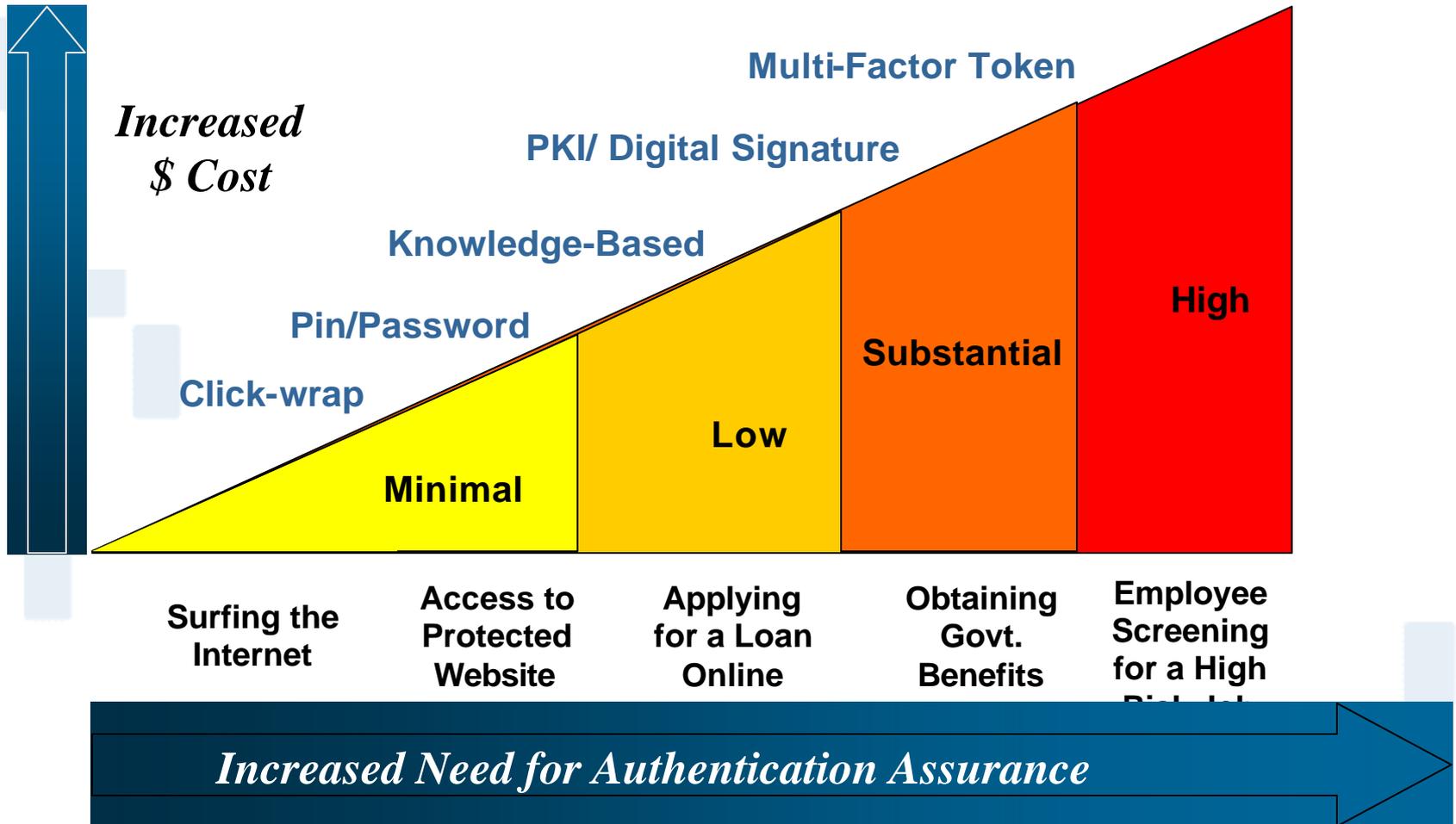
Jay Wack

May 18, 2005

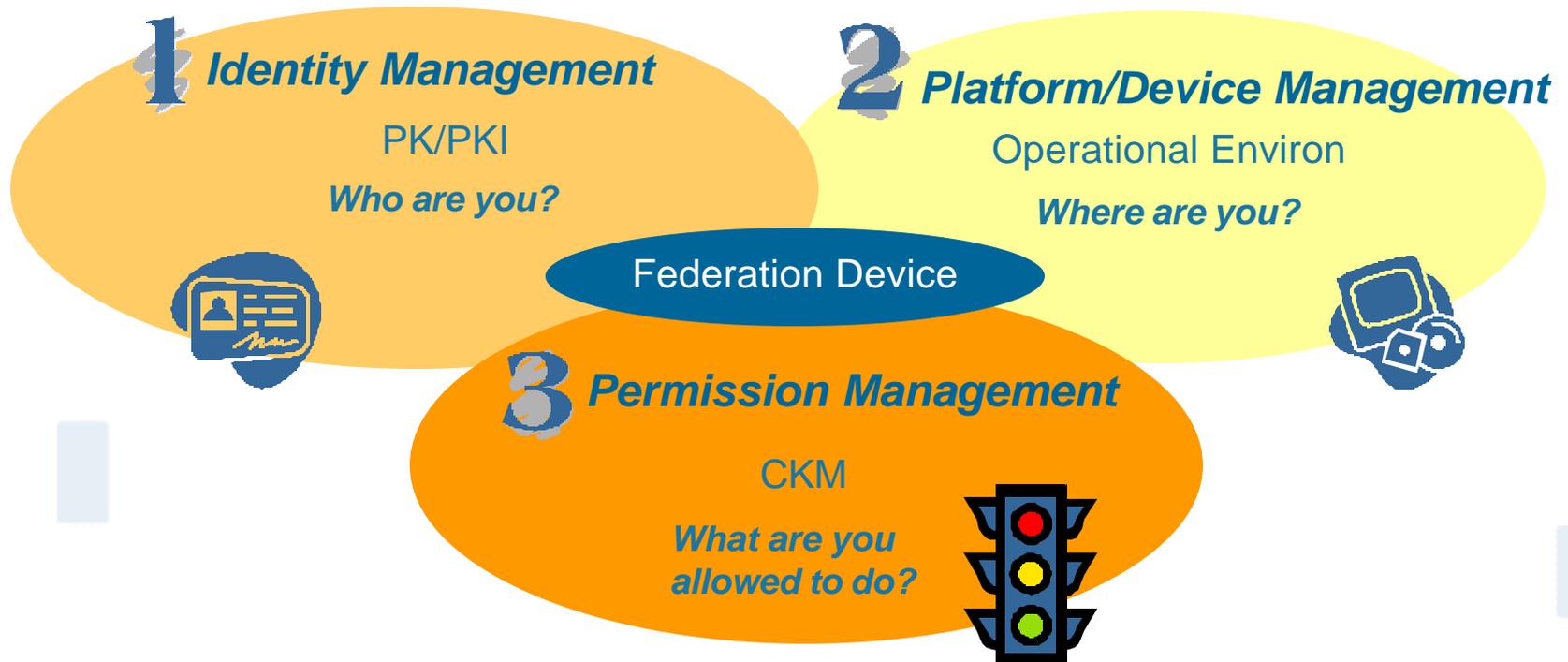
# We Are Connected In Many Ways – Mostly Unexpected



# Authentication Risk and Assurance



# Putting it Together – A Security View



# Secure Communication through Data Protection

---

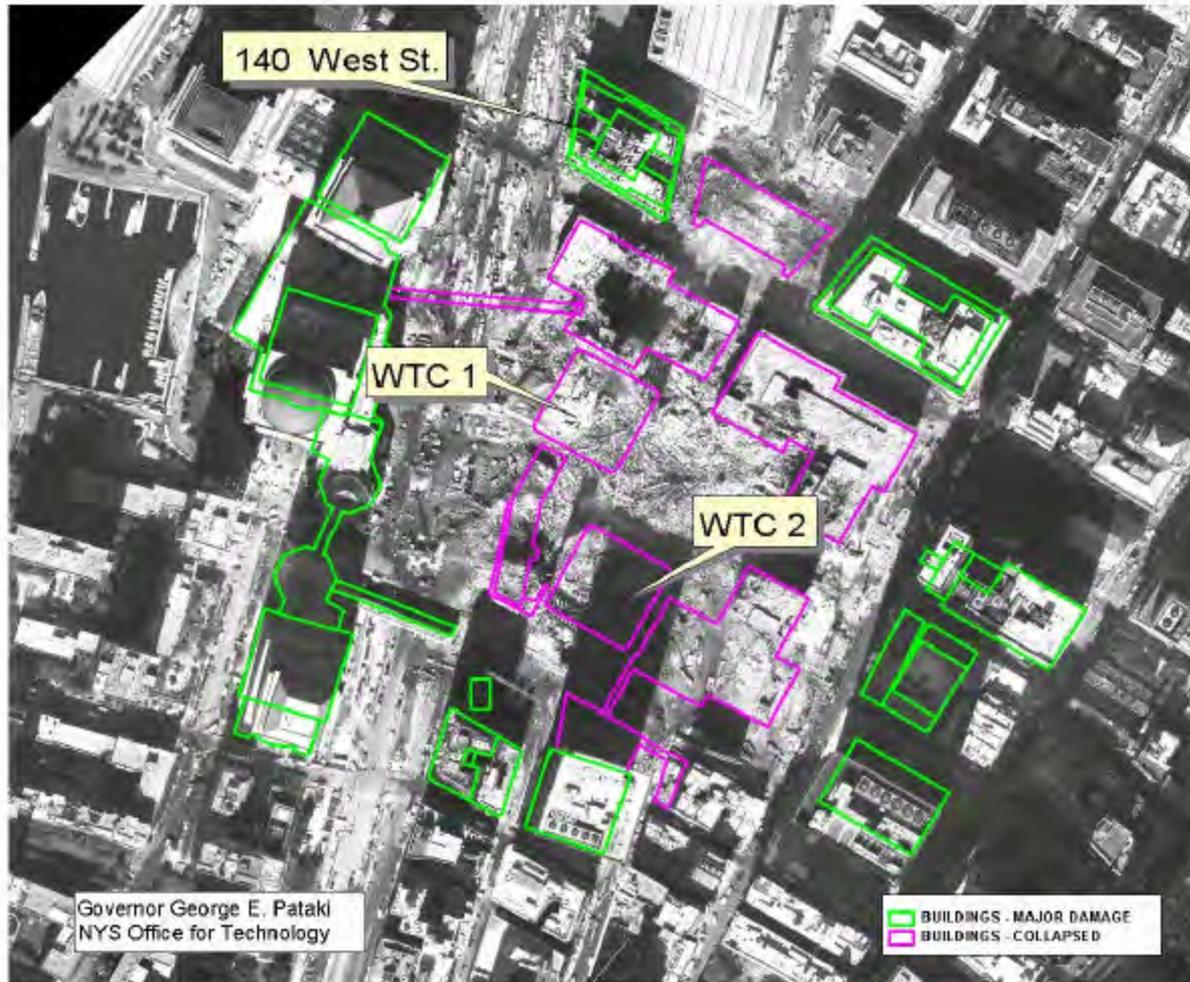
## Individual Characteristics

- **Identity** – Who is this person? What role does he play in the organization? How is he identified (token, biometric, key fob)?
- **Environment** – Where is he? What kind of network connection does he have? What kind of security is on his computer?
- **Authorization** – What is this person allowed to see or do in reference to sensitive information? CKM

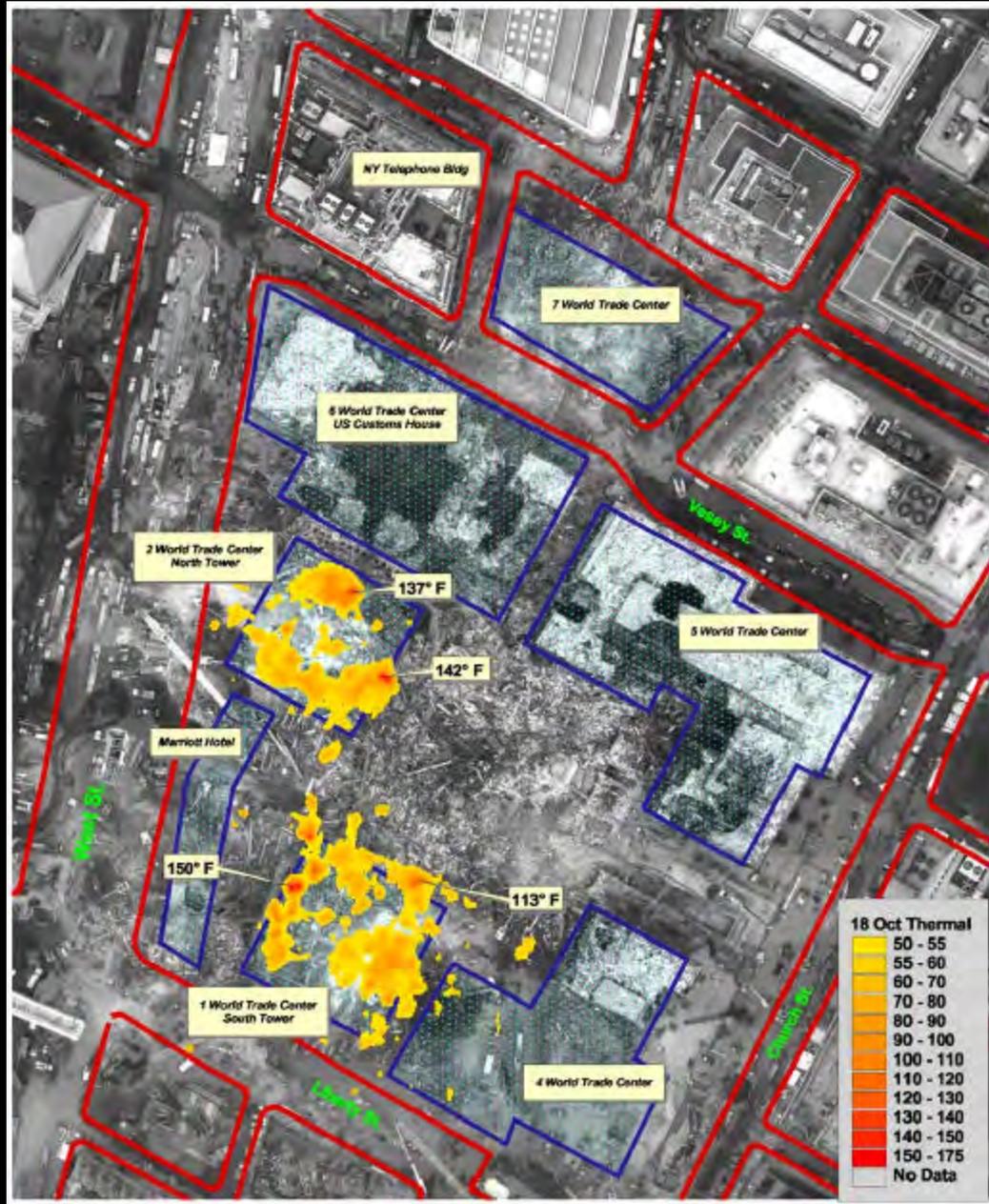
## Data Characteristics

- **Availability** – How easily can the data be accessed?
- **Integrity** – How reliable is the data?
- Where did it come from and has it been altered in any way?
- **Confidentiality** – Are only those authorized to see the data allowed access? Is it protected from everyone else?

***CKM® technology is a, standards-based, cryptographic key management technology that provides role-based access control of information enforced by cryptography.***

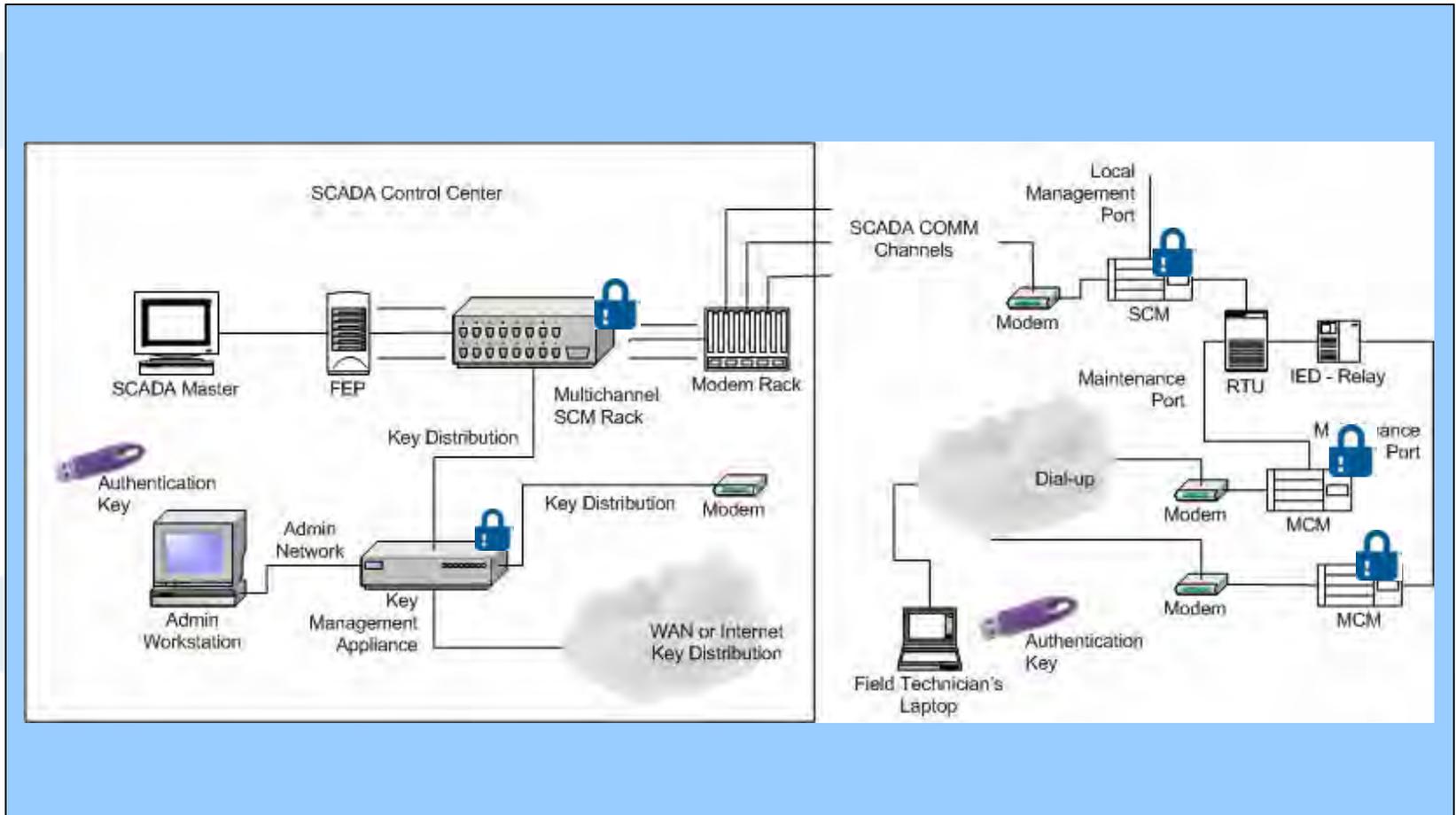


OFT overlaid gas line data with these thermal images to help emergency personnel (in particular, the fire department) determine temperatures relative to gas lines. In addition, NYC overlaid data regarding Freon tanks (for building air conditioning systems) and data regarding fuel tanks.

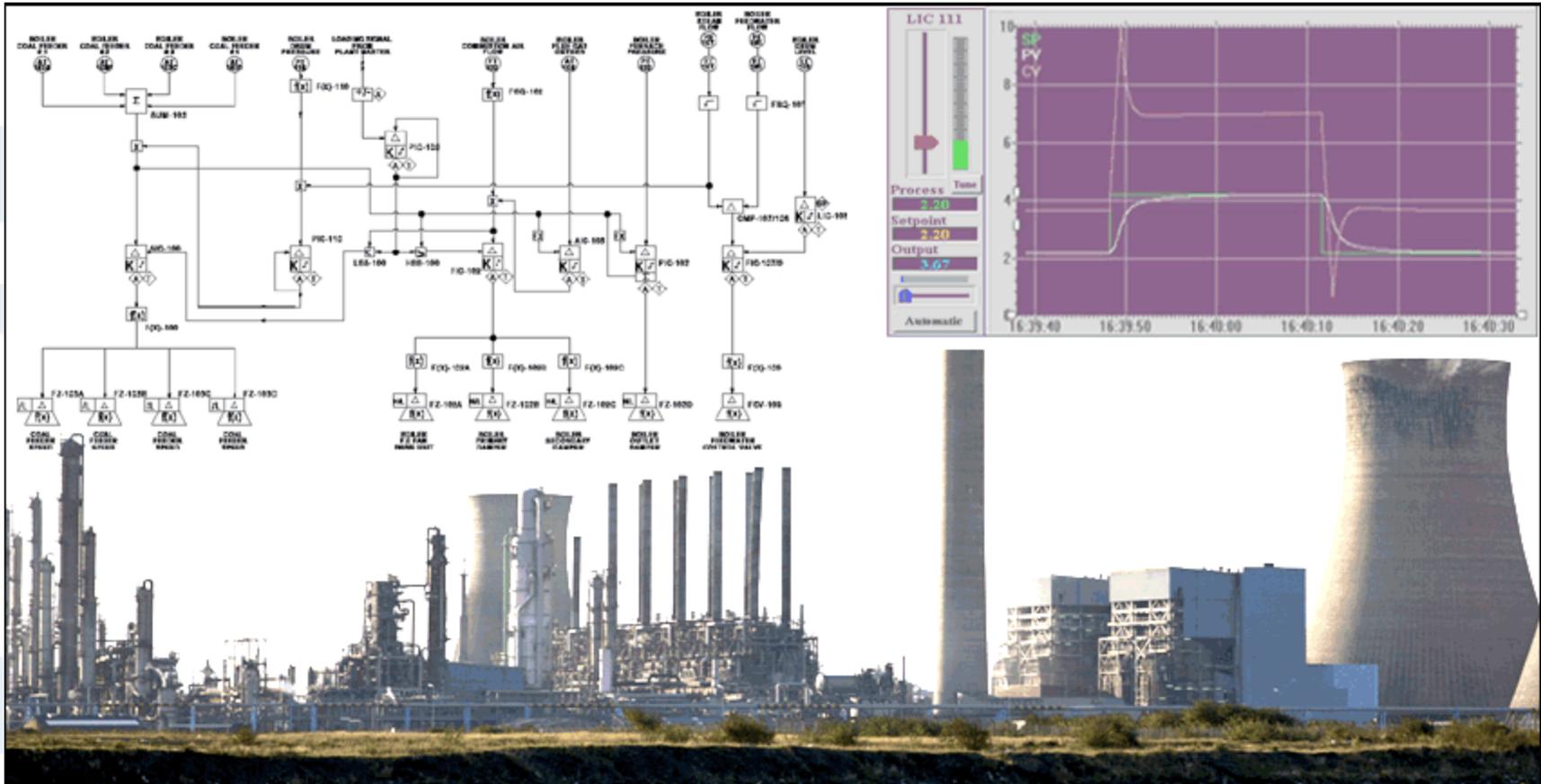


Red lines indicate street outlines; blue lines indicate building footprints.

# A CKM<sup>®</sup> Enabled<sup>®</sup> Cyber Security Solution for SCADA



# What can you see and/or do?





## Components Needed For IA Objectives

---

**COMSEC** is traditional point to point, from here to there.

The network today speaks in terms of “point of presence” – hard to define “there”

**INFOSEC** needs to be protecting the information itself, not the channel.

Information is stored by content, with signatures to provide validation of content.

1. Self Protecting Data Objects
2. Data Label Awareness
3. Data Label Aware Services
4. Identity Management augmented by
5. Key Management That is:
  - Role based
  - Fine Grained (objects)
  - Dynamic, not static, keys

## What is ANSI X9.69? A Process - Called CKM

- CKM, short for Constructive Key Management® technology provides Role Based Access Control that is enforced via cryptography.
- Published as ANSI Standards
  - X9.69 Framework For Key Management Extensions
  - X9.73 Cryptographic Message Syntax
  - X9.96 Secure XML
- Properties of CKM Approach:
  - Key material not specific to individuals
  - Addresses the one-to-many distribution problem of key management
  - Access privileges bound to data via cryptography
  - Built-in key recovery performed by system owner
  - Modeling Role-Based Access Control (RBAC)
  - Content-based security
  - Complementing PKI



# One Document, Different Access Levels (CKM® Word)

*Different sections of this document were encrypted using different Credentials...*



*...and sent over the Internet, Corporate Network, Intranet, Extranet or VPN*

**Internal News Bulletin**

This information is for holders of the US Credential Only



The Luxair turboprop Fokker 50 was flying from Berlin.

Four survivors have been taken to hospital. Emergency workers are trying to free the injured pilot from the wreckage.



**Internal News Bulletin**

**US Citizenship**

**Confidential Classification**

**Medium Threat**



**Internal News Bulletin**

This information is for holders of the US Credential Only



The Luxair turboprop Fokker 50 was flying from Berlin.

Four survivors have been taken to hospital. Emergency workers are trying to free the injured pilot from the wreckage.

The Senior Analyst holds all Credentials and can access the entire document



**Internal News Bulletin**

This information is for holders of the US Credential Only

**Confidential Class**

The Luxair turboprop Fokker 50 was flying from Berlin.

Four survivors have been taken to hospital. Emergency workers are trying to free the injured pilot from the wreckage.

The Junior Analyst does not hold the Confidential Credential and cannot see the image.



**Internal News Bulletin**

[Redacted]

[Redacted]

[Redacted]

Anyone not holding any Credentials can only see the unencrypted information.

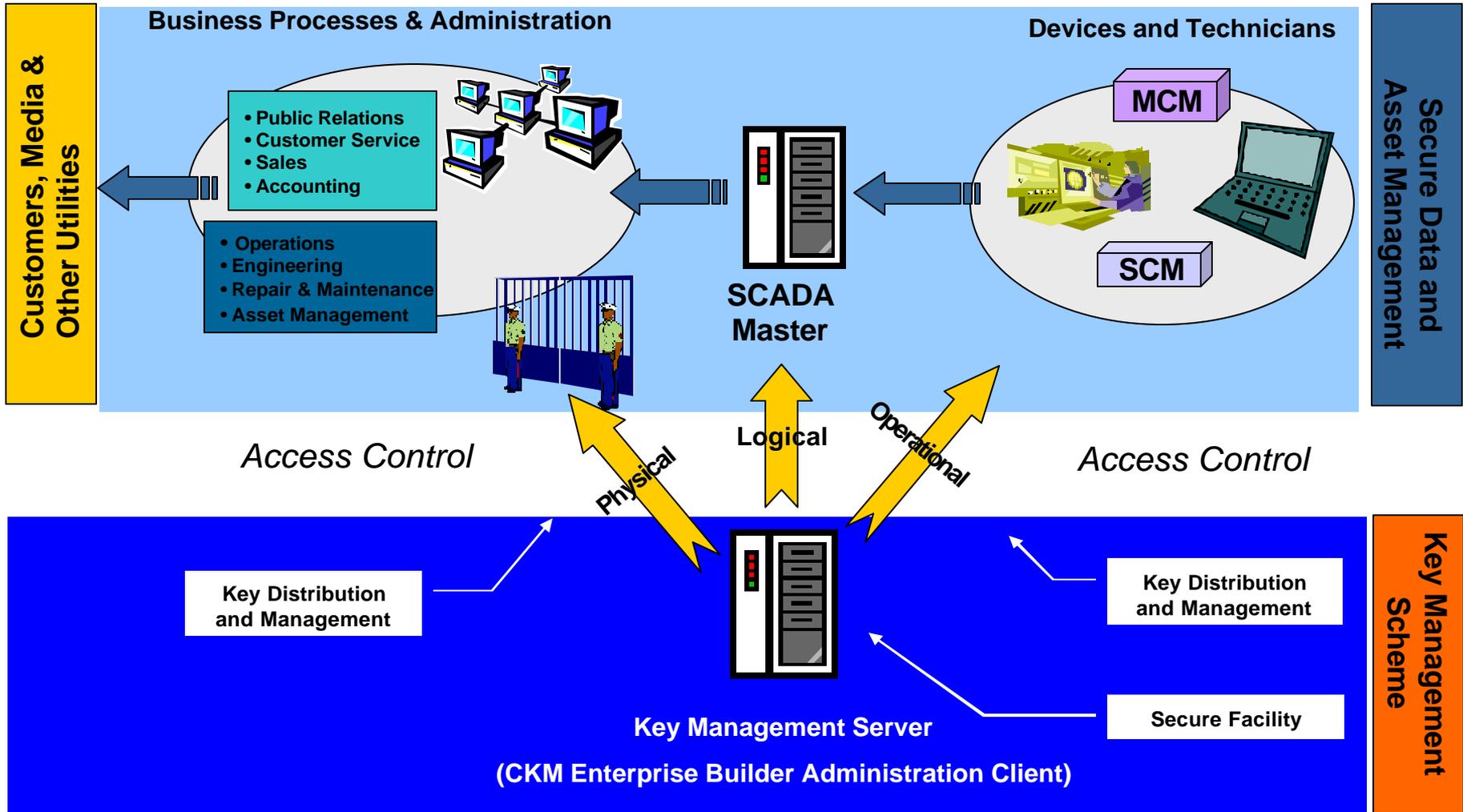


*Note: Users must identify and authenticate themselves to activate their Credentials*

# SCMS<sup>2</sup> for the Utilities Industry

Secure Data and Asset Management

One Overarching Key Management Scheme



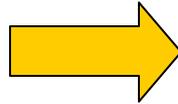
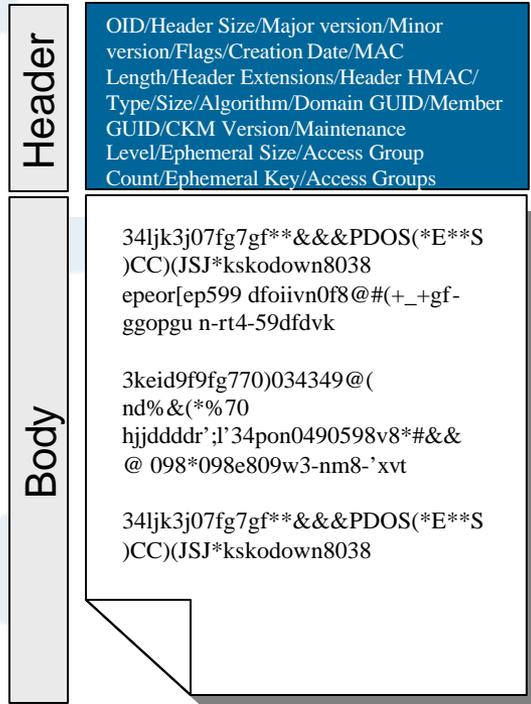
# Permission Matrix

Audience Selector					
01 Intell domain					
1 Classification	2 Non US Class	3 SCI Control	4 SCI Source	5 Dissemination	6 Intell Comm
01 Top Secret	01 NATO	01 BYE	01 Canada S	01 RSEN	01 COMSEC
02 Secret	02 MID East	02 COMINT	02 UK S	02 FOUO	02 SAR
03 Confidential	03 South Am	03 GAMMA	03 Australia S	03 ORCON	03 DIA
04 Unclassified	04 Far East	04 Talent Keyhole>	04 France S	04 NOFORN	04 TTIC
05 Law Enforcement	05 Africa	05 COSMIC	05 Germany S	05 IMCON	05 NSA
06 First Responder	06 Europe	06 ATOMAL	06 Japan S	06 FRD	06 CIA
07 Local Government	07 UN	07 GAMMA	07 France S	07 CNMDI	07 DoD
08 Controlled	08 Canada	08 Restricted	08 UK TS	08 SAMI	08 Critic
02 Business domain					
1 Planning	2 Installations	3 Logistics	4 Human Resources	5 Acquisitions	6 Operations
01 Strategic	01 Base	01 Movement	01 Skill Set	01 Materials	01 POM
02 Operational	02 Post	02 Condition	02 Rank	02 Strategic	02 OM
03 Tactical	03 Station	03 Disposition	03 Benefits	03 Info Syst	03 Strategic
04 Business	04 Camp	04 Supply Levels	04 Health	04 Ammunition	04 Supplemental
05 Financial	05 Facility	05 In Transit	05 Training	05 Weapons	05 Contingency
06 Budgetary	06 Mobile	06 Merged View	06 Recruiting	06 Foods	06 Programmatic
07 Logistical	07 Deployed	07 Total Assets	07 Dependents	07 Fuels	07 Budgets
08 Facilities	08 Depot	08 COP	08 Aggregate	08 Clothing	08 Planning
03 War Fighter domain					
1 Audience	2 Type	3 Content	4 Organization	5 Battlespace Aware	6 DOC Aware
01 Allied Forces	01 C3I	01 ELINT	01 Army	01 Threats	01 WMD
02 Allied Forces N	02 C2IS	02 EW	02 Navy	02 Time Latency	02 Counter Terror
03 NATO	03 INTEL	03 GIS	03 Marines	03 EOB	03 Info Ops
04 Regional Coalition	04 OPCON	04 HUMINT	04 Seals	04 Friendly	04 Urban Ops
05 Joint Task Force	05 SyOps	05 IEW	05 Air Force	05 Reserves	05 MOOTW
06 Combined JTF	06 C4SRI	06 IMINT	06 Coast Guard	06 Operations	06 Targeting
07 UN	07 HRM	07 SIGINT	07 Nat Guard	07 Strike Mission	07 I and W
08 US Only	08 Medical	08 Biological	08 Reserves	08 Imagery	08 Space and Undersea

Commit

# CKM Object and Header

## CKM Encrypted Object



## CKM Header Details

OID/Header Size/Major version/Minor version/Flags/Creation Date/MAC Length/Header Extensions/Header HMAC/Type/Size/Algorithm/Domain GUID/Member GUID/CKM Version/Maintenance Level/Ephemeral Size/Access Group Count/Ephemeral Key/Access Groups

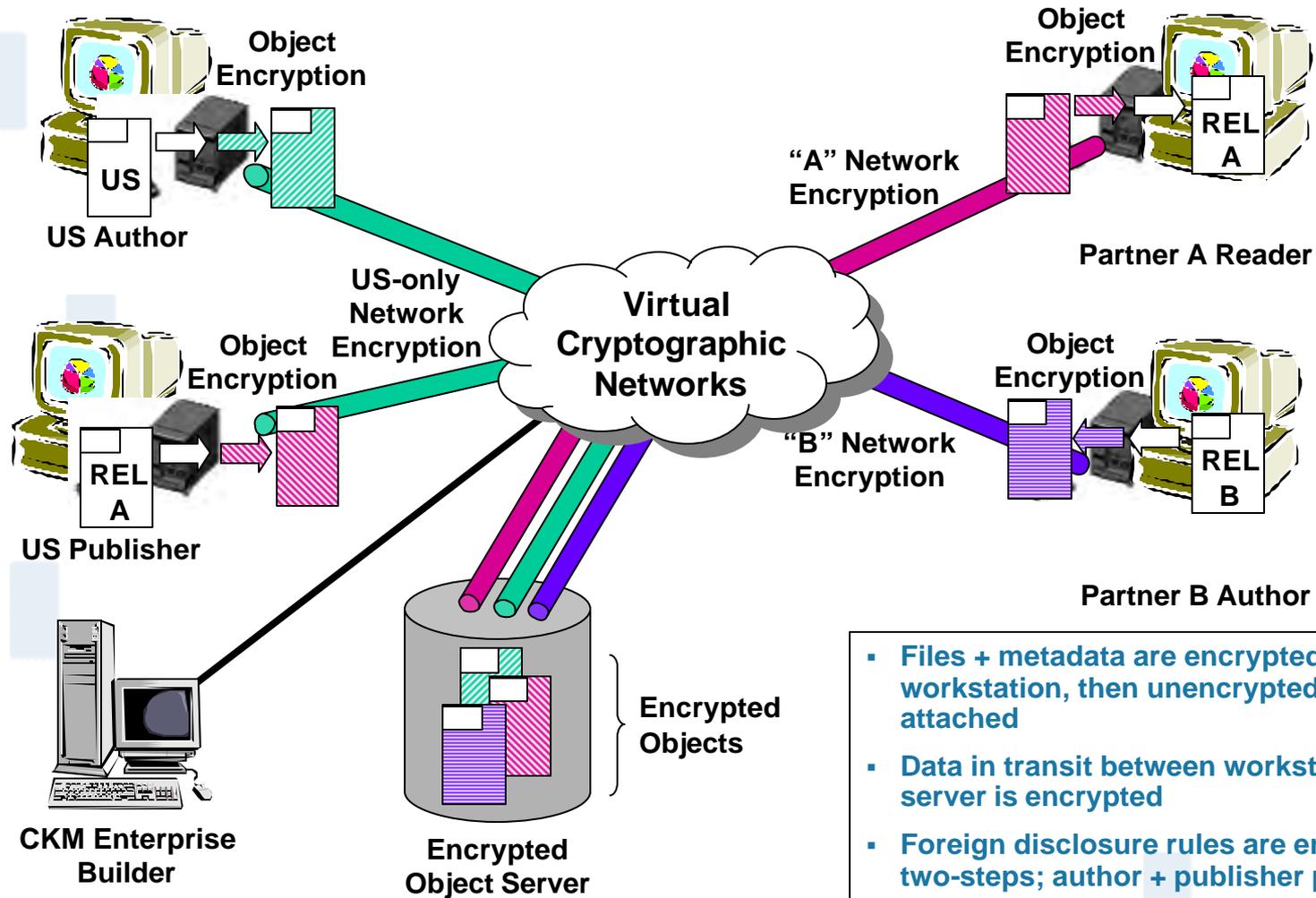
And looks like this.....

```
2.23.42.9.10.3.0.3.0  D  °
                        B
                        ±
{çIi;/S±»Vã±-TYÖGã2.23.42.9.10.3.0.2.0
20050218193459Z  •  É  -  ûý-l(L';{a—
eâlJšđ>6'ÑO—D§  @Öðÿ  €  ³  æÓ¼  -
,riv÷L  ñ{@q  èÚÖðÒ} F  ÚZø<Æ+n•  ^  %&{  İ  Ä
Đ>“Á  •  !âOÿ×,ä  fñzÜ  9  æP  ÿÖë>yP,,Ä®
```



Shows Pointers in Header

# CKM Overview – Community of Interest Networks

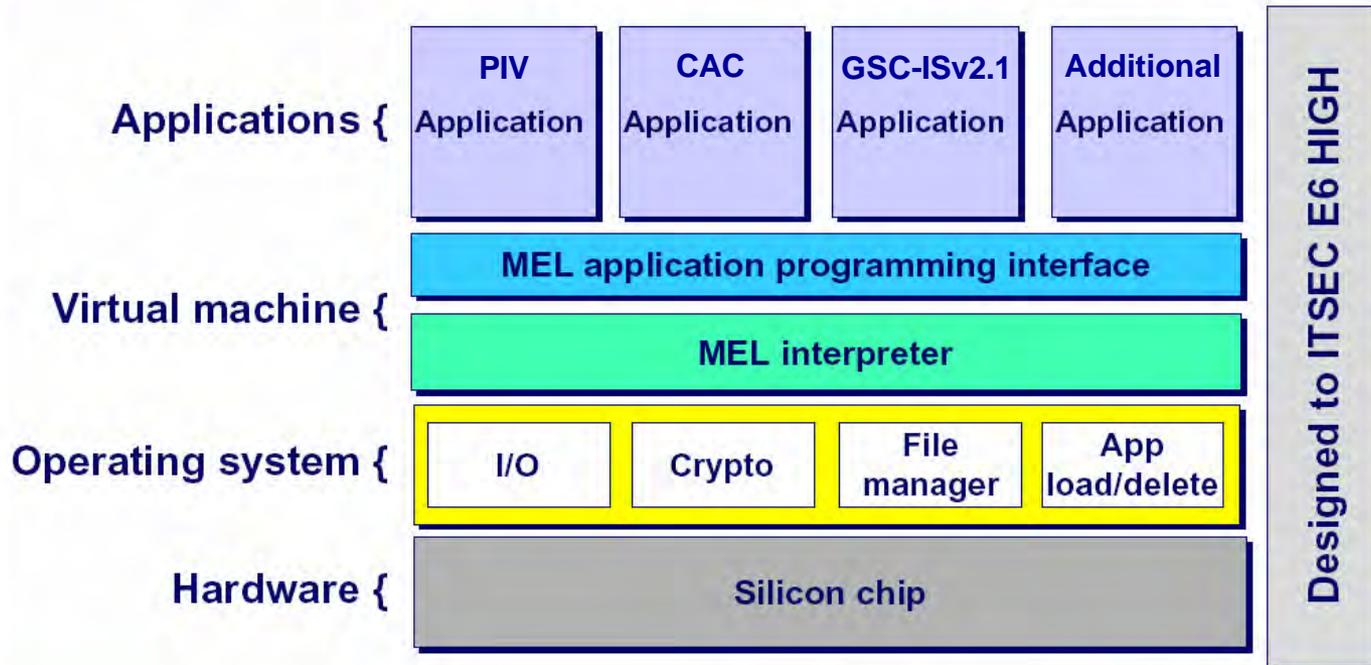


- Files + metadata are encrypted on the workstation, then unencrypted metadata is attached
- Data in transit between workstations and server is encrypted
- Foreign disclosure rules are enforced via two-steps; author + publisher processes

\* Network only encryption (data in transit)

# MULTOS Operating System

## MULTOS : Multi-Application Operating System

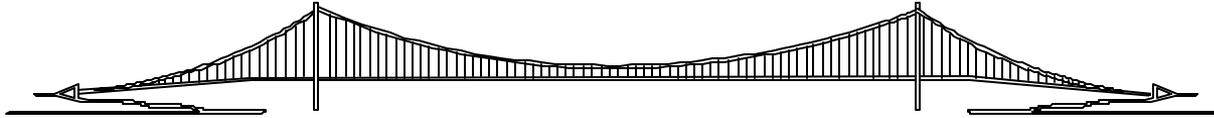


© MAOSCO Limited 2000

**MULTOS**

## Smart Card with Cryptography

The Smart Card with Cryptography Is a Bridge for Application Integration & Increases the Use of Existing Investments



### MULTOS Cards w/ Constructive Key Management

#### Existing Tools

- VPN
- SSL
- IPSEC
- Other Proprietary solutions



#### Infrastructure

- Internet - Gates
- LAN-WAN - Doors
- Intranet - Windows
- Enterprise - Data
- Dial-ups - Functions
- Desktops - Images
- Laptops - Content



#### CKM with MULTOS

- Multiple Security Levels
- Cryptographic mediation
- Hardware Independence
- Network Independence
- Data Recovery
- Future & Legacy Systems
- Low Cost
- Object Oriented



## Contact Info

---

Jay Wack

TecSec® Incorporated

[jayw@tecsec.com](mailto:jayw@tecsec.com)

703 744 8447