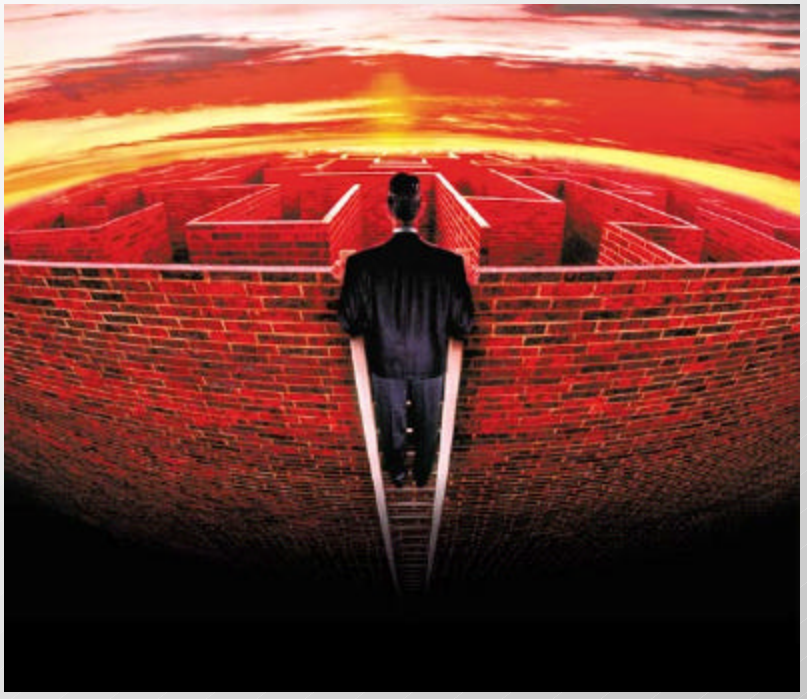


Release Management with Label Security in Large Scale Digital Libraries

Jack Wool
jwool@cryptek.com
Cryptek, Inc.

Introduction

- Release management has evolved to providing content management throughout the workflow lifecycle
  - Not just a boundary issue
- Content handling policy is dynamic
- Subscribers are dynamic in location, data rights, role, etc
- The full lifecycle covers source, transport, and post receipt management
- Cryptek is evolving from a MLS transport management (Distributed B2 network system) to secure content distribution management.
- Policy flexibility is a key component of dynamic response to operational requirement

Cryptek®

Introduction

- DiamondTEK is designed upon the “RedBook” B2-level Community of Interest (COI) NSA secure network model.
- Derivative of network security product on the NSA’s evaluated product list at the B2 level of trust (VSLAN-DiamondLAN).
- The B2 rating signified that DiamondLAN had the level of trust required to allow multiple levels of classification to occupy a single network without allowing information from a higher level to seep to a lower one.
- The implementation uses data labeling at the packet level as one of the optional methods for “marking” data in motion.
- Mandatory enforcement methods use label/policy/location/role matrix for gating decisions.

Cryptek®

Baseline Product Snapshot

- Distributed Network Security Appliances –"Diamond*TEK*™"
  - EAL4, FIPS-140, FIPS-188
  - B2 red book product heritage
- Dynamic Secure Virtual Networks (DSVN™) within a single network infrastructure.
- Integration of technology into Thin Client Stations
  - Ex: DiamondUTC (Secure SunRay)
- System Integration in Large Scale Document Management Systems for Military Logistics
- Inside/out, policy driven, content object view of security.
- Drop-in network security appliance.

Cryptek®

Security Pedigree Product History

EAL 4 Certified 2002

1985 - 1989 | **1990 - 1995** | **1996 - 2000**

Jan 1985
VSLAN Development Started

Oct. 1985
First Company to Enter B2 Evaluation For Network Product

March 1987
VSLAN 1.0 Released

August 1987
VSLAN 2.0 Released

March 1988
VSLAN 3.0 Released

Jan. 1989
VSLAN 4.0 Released

March 1990
VSLAN 5.0 Released

August 1990
B2 Certification Received. For VSLAN 5.0 First and Only Company to achieve this level

January 1994
RAMP Certification for VSLAN5.1

July 1995
RAMP Certification for DiamondLAN 6.0

March 1997
Migration from VSLAN to DTEK Started

June 1997
Enter RAMP for B2 Certification of DTEK

Sept. 1999
DiamondTEK V1.0 Released

March 2000
DiamondTEK Moved from TPEP B2 to Common Criteria

July 2000
DiamondTEK V2.0 Released

Cryptek®

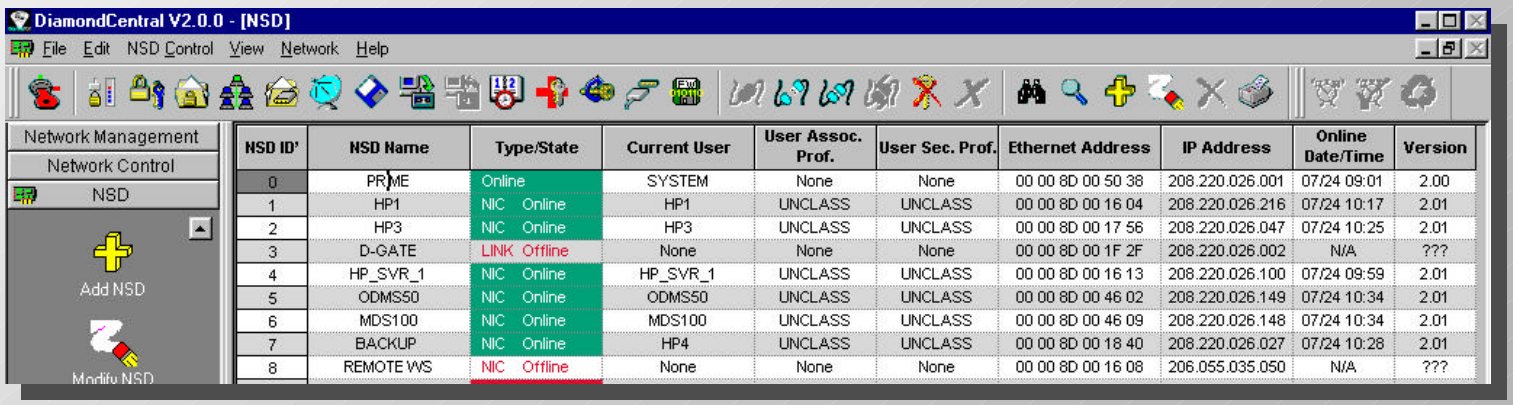
Common Criteria Compatibility Map

Common Criteria	US-TCSEC	European ITSEC
	D: Minimal Protection	E0
EAL1		
EAL2	C1: Discretionary Access Control	E1
EAL3	C2: Controlled Access Protection	E2
EAL4	B1: Labeled Security Protection	E3
EAL5	B2: Structured Protection	E4
EAL6	B3: Security Domains	E5
EAL7	A1: Verified Design	E6

Cryptek®

Policy Creation and Management Network View

- Define user-specific security profiles
  - Authorization rules
  - Service Filtering rules
  - IP Filtering rules
  - Communications rules
- Users may be allowed to use multiple profiles
- Policies are dynamically deployed to system devices
- Uniform policy enforcement independent of systems and users
- Upgrades device firmware over the network
- Maintains audit logs and keys

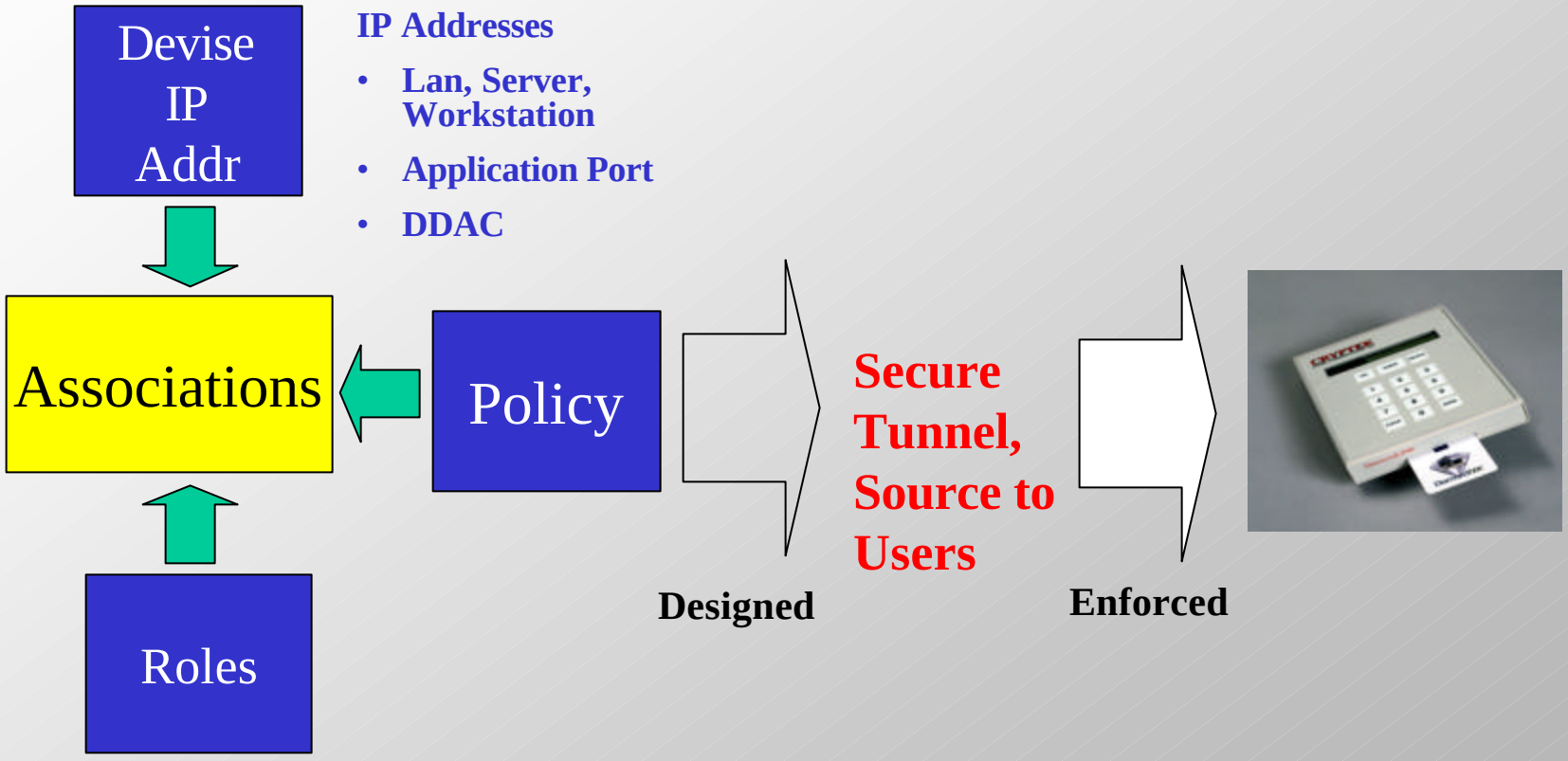


NSD ID'	NSD Name	Type/State	Current User	User Assoc. Prof.	User Sec. Prof.	Ethernet Address	IP Address	Online Date/Time	Version
0	PRIME	Online	SYSTEM	None	None	00 00 8D 00 50 38	208.220.026.001	07/24 09:01	2.00
1	HP1	NIC Online	HP1	UNCLASS	UNCLASS	00 00 8D 00 16 04	208.220.026.216	07/24 10:17	2.01
2	HP3	NIC Online	HP3	UNCLASS	UNCLASS	00 00 8D 00 17 56	208.220.026.047	07/24 10:25	2.01
3	D-GATE	LINK Offline	None	None	None	00 00 8D 00 1F 2F	208.220.026.002	N/A	???
4	HP_SVR_1	NIC Online	HP_SVR_1	UNCLASS	UNCLASS	00 00 8D 00 16 13	208.220.026.100	07/24 09:59	2.01
5	ODMS50	NIC Online	ODMS50	UNCLASS	UNCLASS	00 00 8D 00 46 02	208.220.026.149	07/24 10:34	2.01
6	MDS100	NIC Online	MDS100	UNCLASS	UNCLASS	00 00 8D 00 46 09	208.220.026.148	07/24 10:34	2.01
7	BACKUP	NIC Online	HP4	UNCLASS	UNCLASS	00 00 8D 00 18 40	208.220.026.027	07/24 10:28	2.01
8	REMOTE WS	NIC Offline	None	None	None	00 00 8D 00 16 08	206.055.035.050	N/A	???

Diamond*Central* Network Security Controller

Cryptek®

Securely manage and transport data



Role-based Policy
DiamondCENTRAL

IPSec Appliances
DiamondTEK Family

Cryptek®

Data Driven Access Control (DDAC™)

- Data Driven Access Control (DDAC™) labels sensitive proprietary data and those labels determine where specific data can and cannot go.
- The network infrastructure and data collaborate to control data transfer and offer the highest level of security available.
- Provides a security processor embedded into network appliances.
- The self-protecting security computer is dedicated to enforcing network security policy and includes security functions that prevent subversion by malicious users, network attacks, and operating system flaws.

Cryptek®

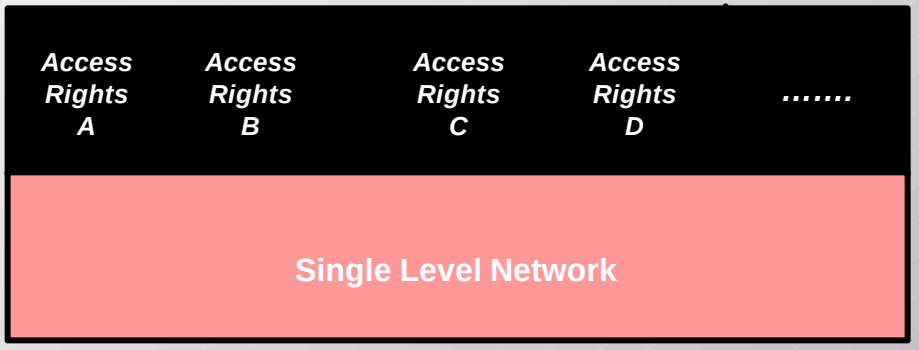
Packet Labeling

Policy-driven content tags provide security-based separation on single physical networks

Redefinable On-the-Fly

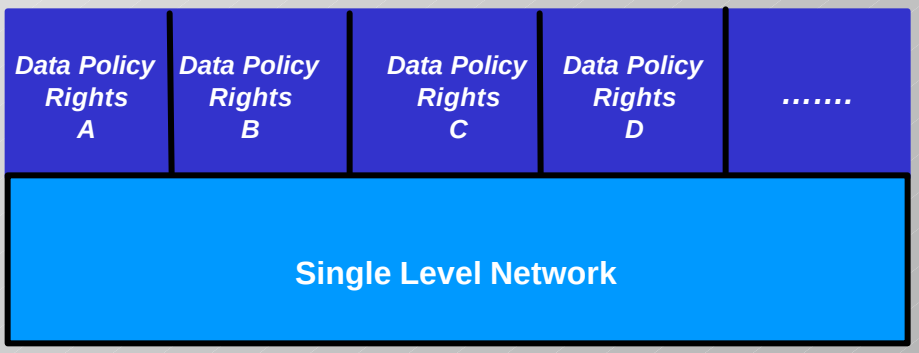
Dynamic Secure Virtual Networks

DSVN



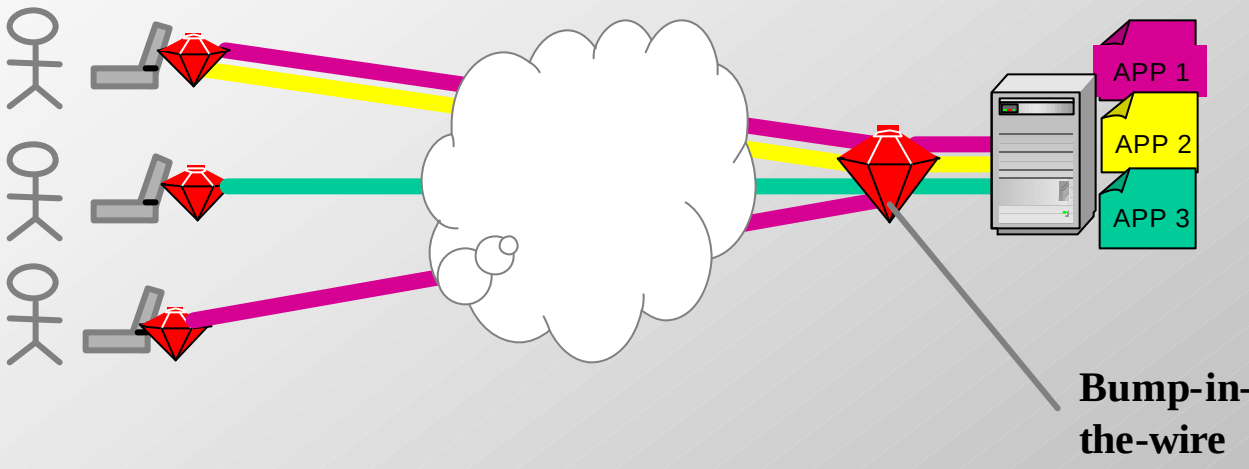
Data-Driven Access Control

DDAC



Cryptek®

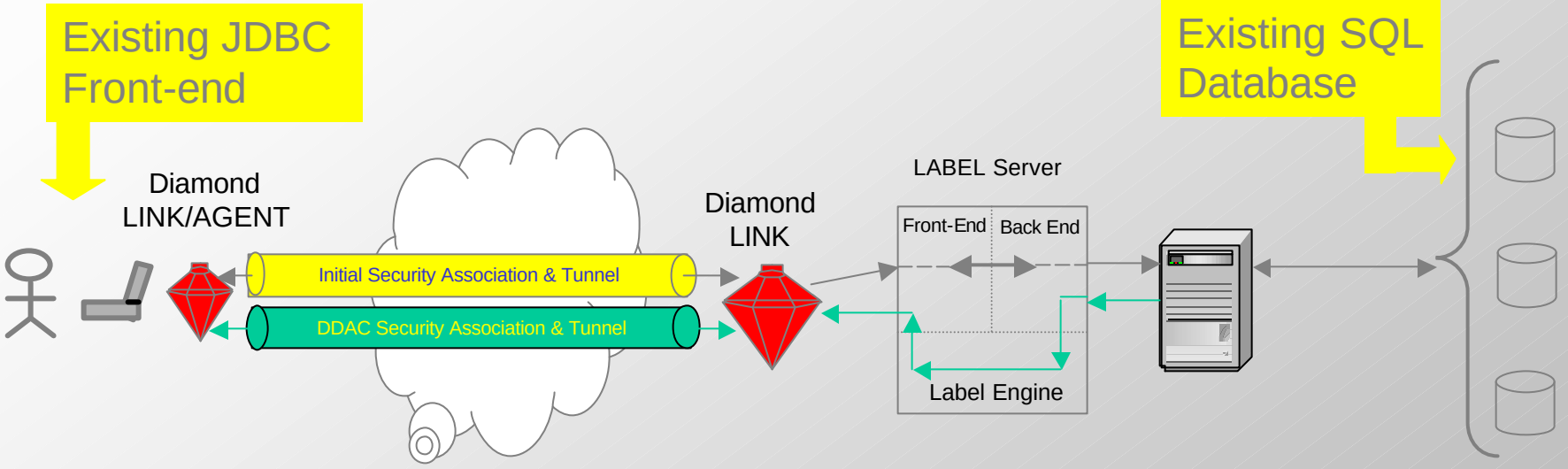
Step 1
Application Access Control



- Application Access Security and Transmission Security is deployed outside the server and/or application
- NO modifications to the Application, Server or Client required
- Full-path (end-to-end) security is provided
- Access Control is driven by the application being accessed not the network or server

Cryptek®

Step 2
Data Driven Access



STEP 1: Initial Access, Authorization and Tunnel is established based on base Security Policy

STEP 2: SQL Queries established with existing database go through the Label Server. Label Servers includes “required field(s)” with Query.

STEP 3: Label Server creates FIPS 188 label based on returned contents of “required fields”

STEP 4: Specific Data Driven Access, Authorization and Tunnel created based on FIPS 188 label generated from query. DiamondLINK accepts or rejects DB row.

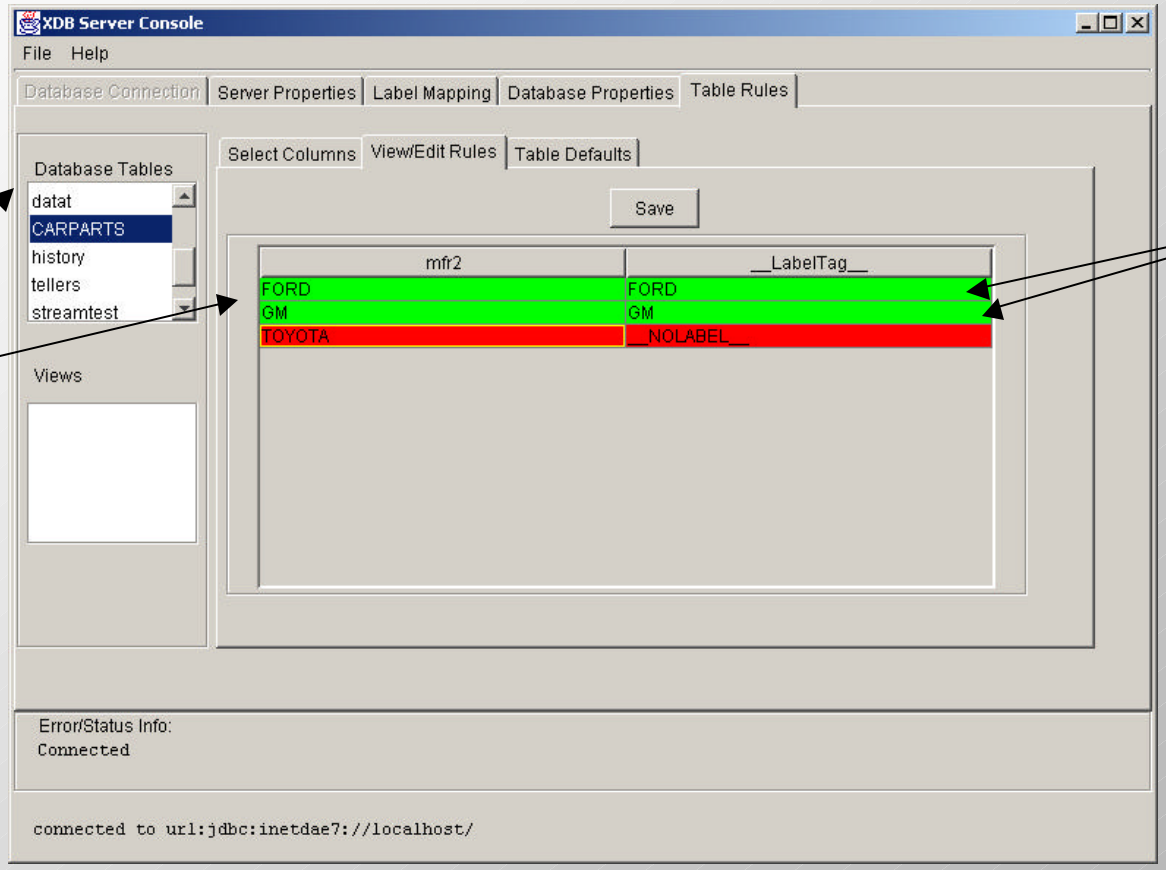
Cryptek®

DiamondVDL Features Application Example

- *Fine-Grain Access Controls through Policies*
- Ease of System Management of Dynamic Environments
  - Imports and Auto-Catalogs - Schemas & Data Values
  - *Point and Click* configuration of Security Policy
  - Access Controls – Distribution Lists
  - Programmable Defaults – Actions to undefined policies
  - Policy changes independent of DB schema or content
- Audit
  - Bad query patterns for tuning
  - Anomalies as potential malicious attempts
- Query Access using *JDBC (ODBC next)* open interfaces
- Total Network Enforcement
- Coalition Network Architecture

Cryptek®

Policy Configuration

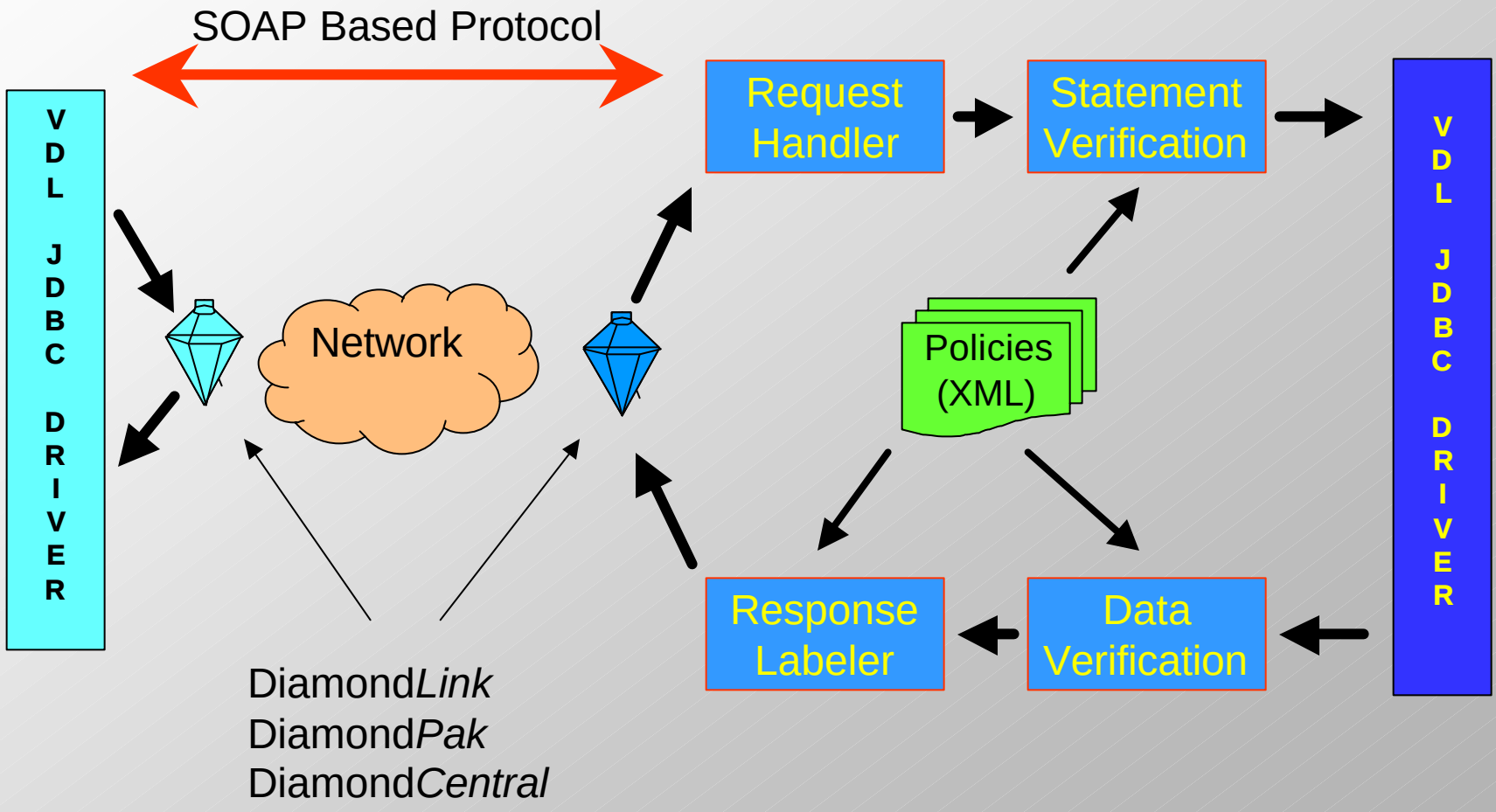


Imported Schema & Domains

Policy Setting

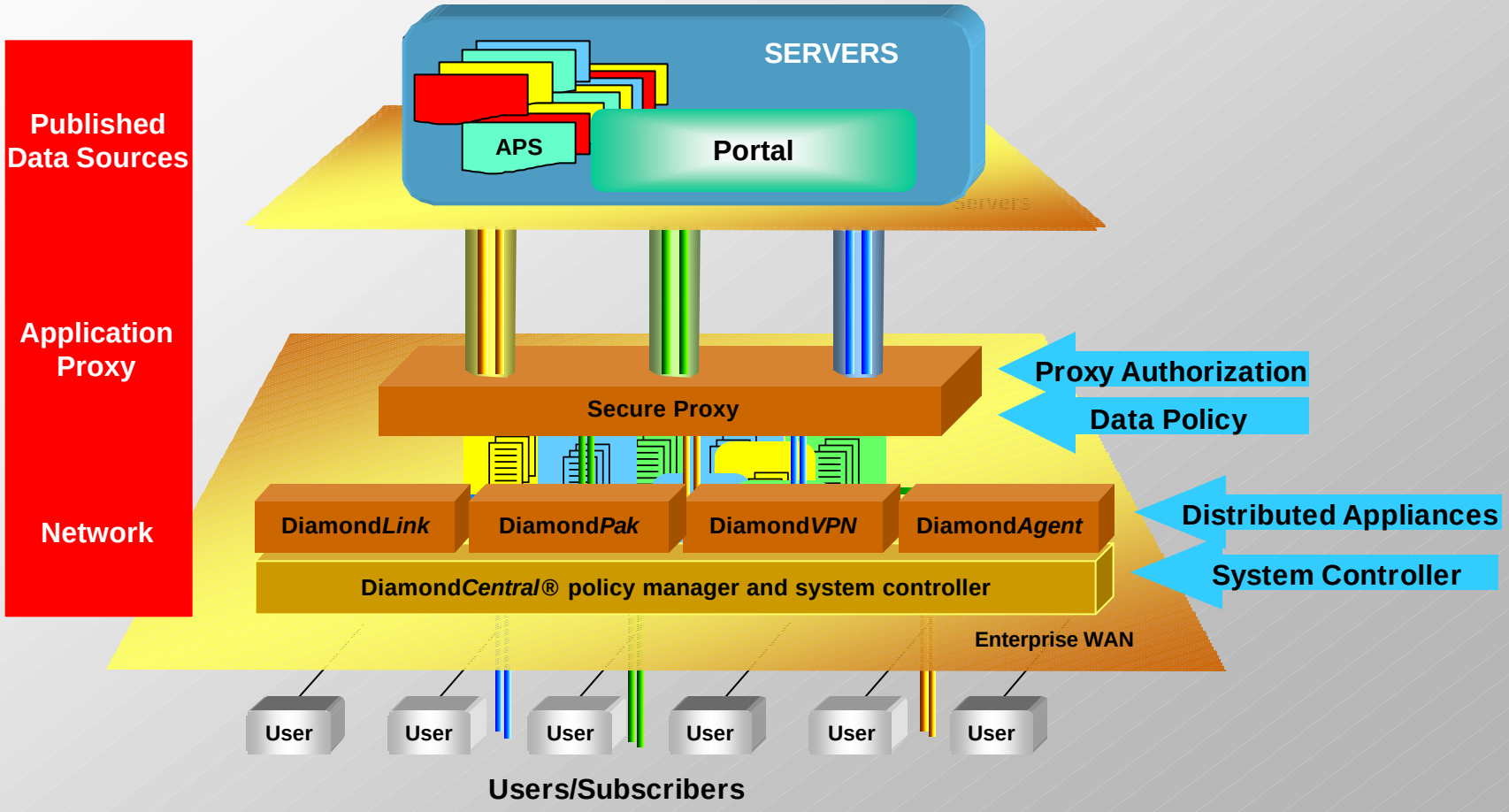
Cryptek®

Key Architectural Components



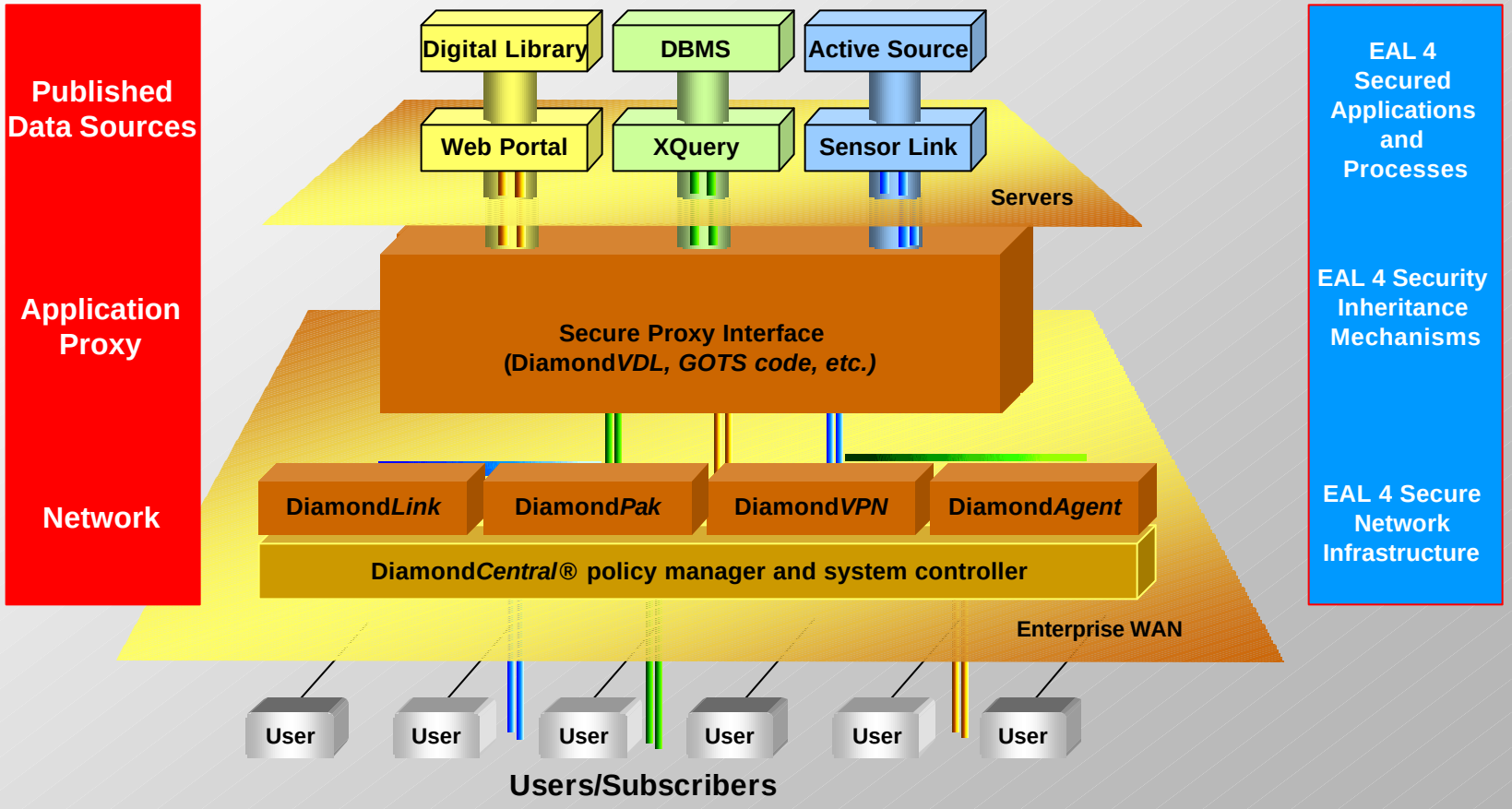
Cryptek®

Composed System



Cryptek®

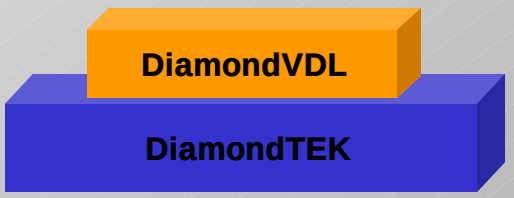
EAL 4 Certification Inheritance
(Work in Progress Issue)



Cryptek®

Common Criteria Inheritance
(Work in Progress Issue)

- Building block approach to system composition allows high assurance attributes to be inherited by protected systems
  - A subset of assertions can be propagated
- DiamondTEK system provides EAL4 security functions for network based systems (e.g. DiamondVDL)
  - User identification and authentication
  - Mandatory access control policy for users
  - Auditing for authenticated users
  - Network protection for servers and clients
  - Application access protection
  - Role based communications channels



- Allows snap-on to distributed architectures with some assertions sustained for the composed architecture.

Cryptek®

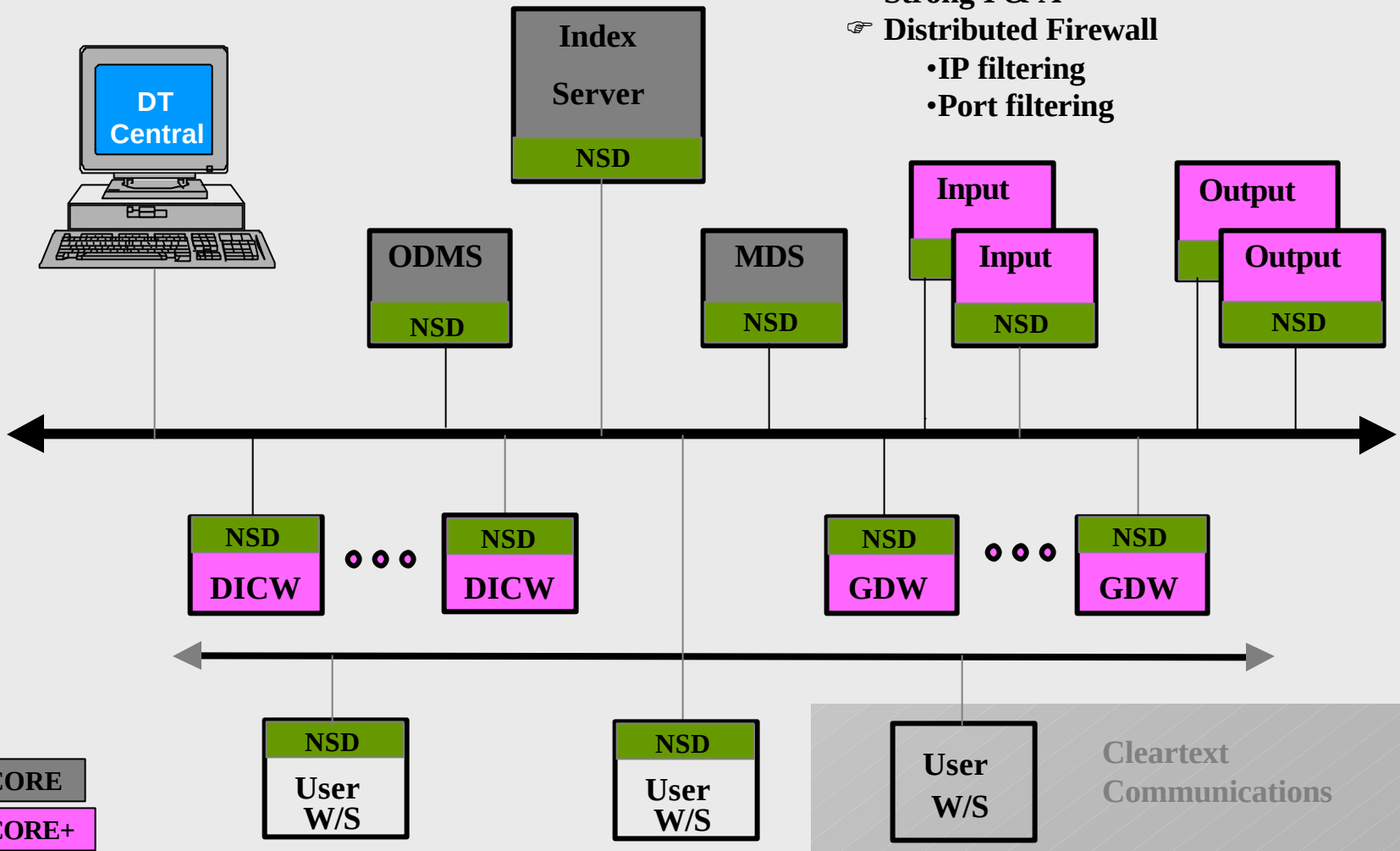
Case Study – JEDMICS
Joint Engineering Data Management and Control System

- Asset value of information: $23B
- Information storage sites: 32
- Total users: > 30,000
- Diamond*TEK* provides three levels of centrally controlled access
  1. Harden core servers and administrator workstations to hide servers and administrators from hacking probes
  2. Secure on-site user communities to hide sensitive data on shared corporate infrastructure
  3. Secure remote Internet access by suppliers while ensuring competitors cannot access supplier data

Cryptek®

Securing JEDMICS

- Encryption between Core+ nodes
- Strong I & A
- Distributed Firewall
  - •IP filtering
  - •Port filtering



Cleartext Communications

Cryptek®

WebJEDMICS Architecture

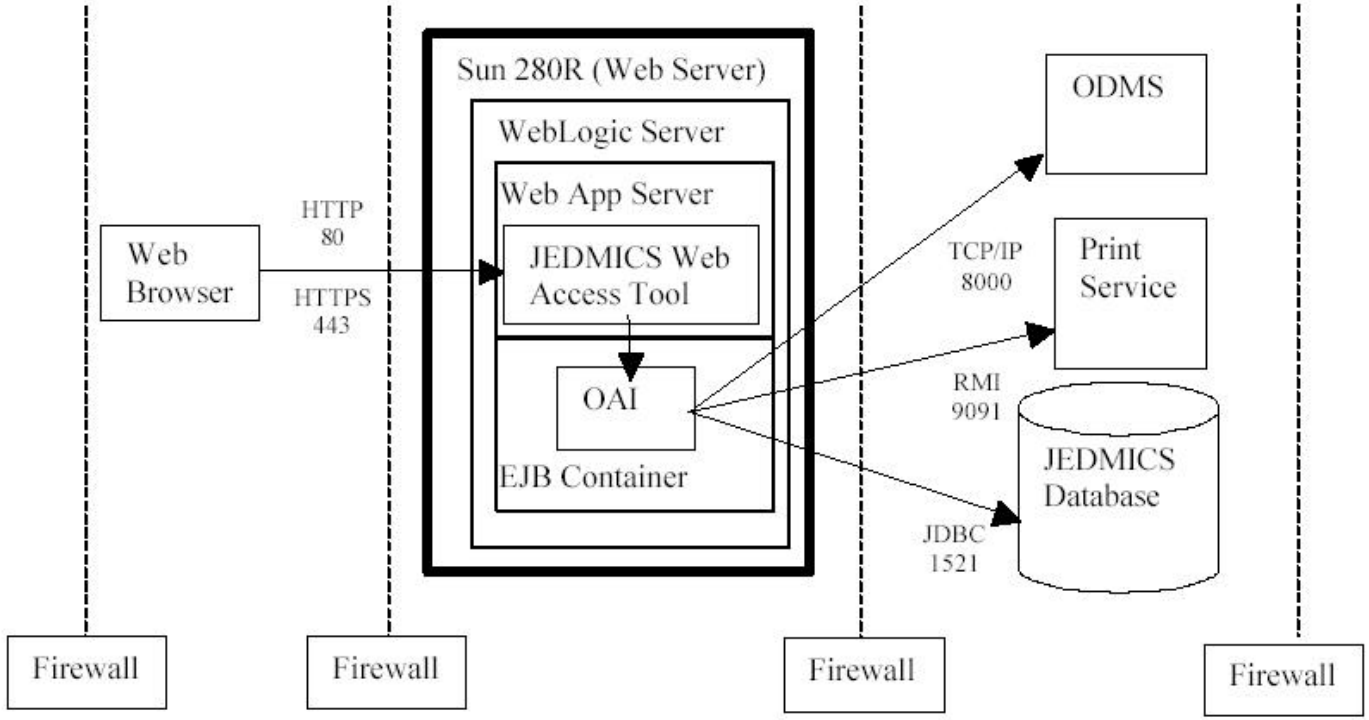


Figure 1 - WebJEDMICS System Architecture

EJB – Enterprise Java Beans
OAI – Open application Interface

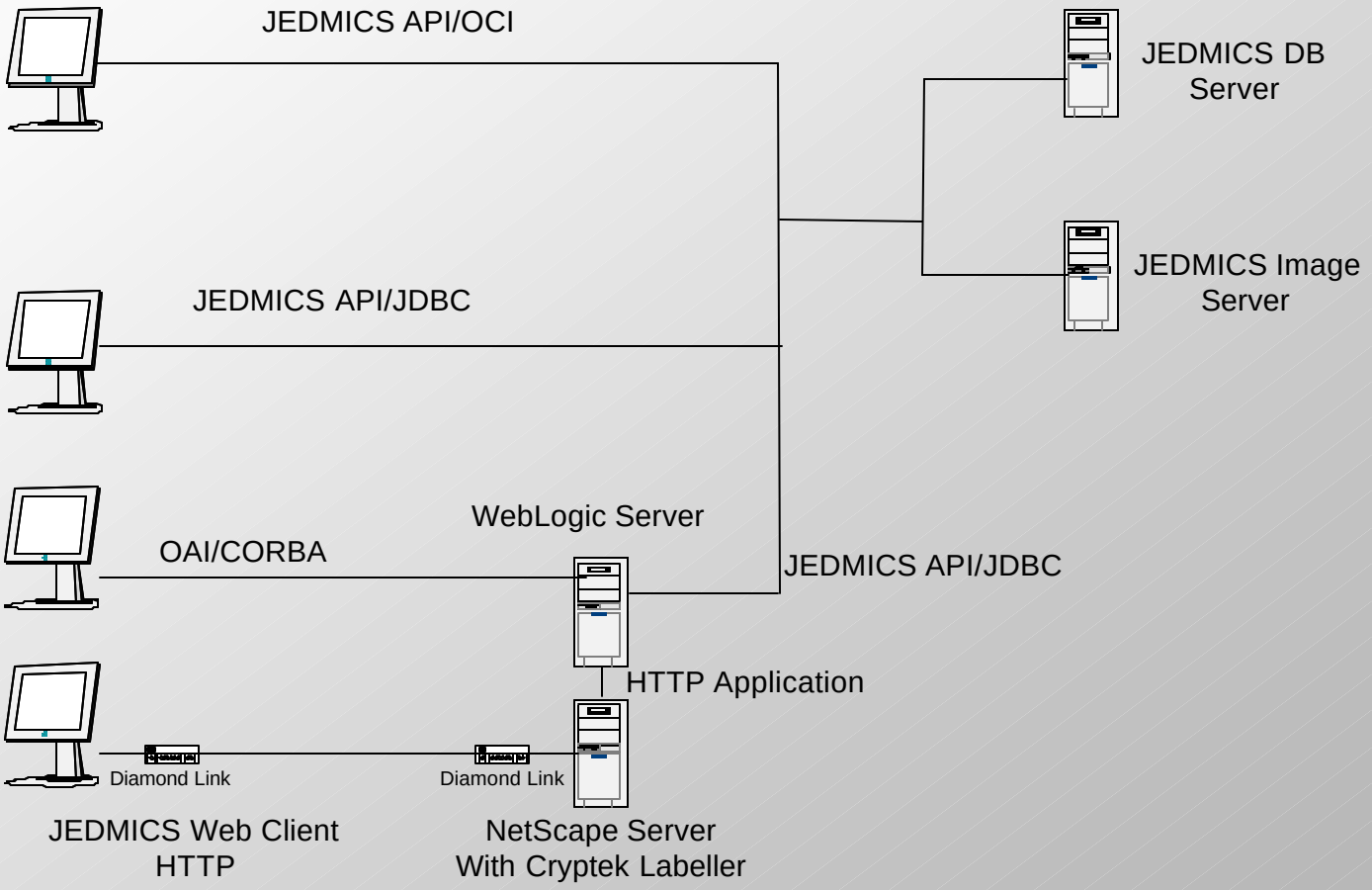
Cryptek®

Diamond*Pod*™ Secure Data Management Platform

- Secure EAL 4 environment
- Redundant security components pre-wired and ready for operation
- Internal data flows are encrypted
- Router and UPC preinstalled
- Applications servers integrated

Cryptek®

Label Server Demonstration



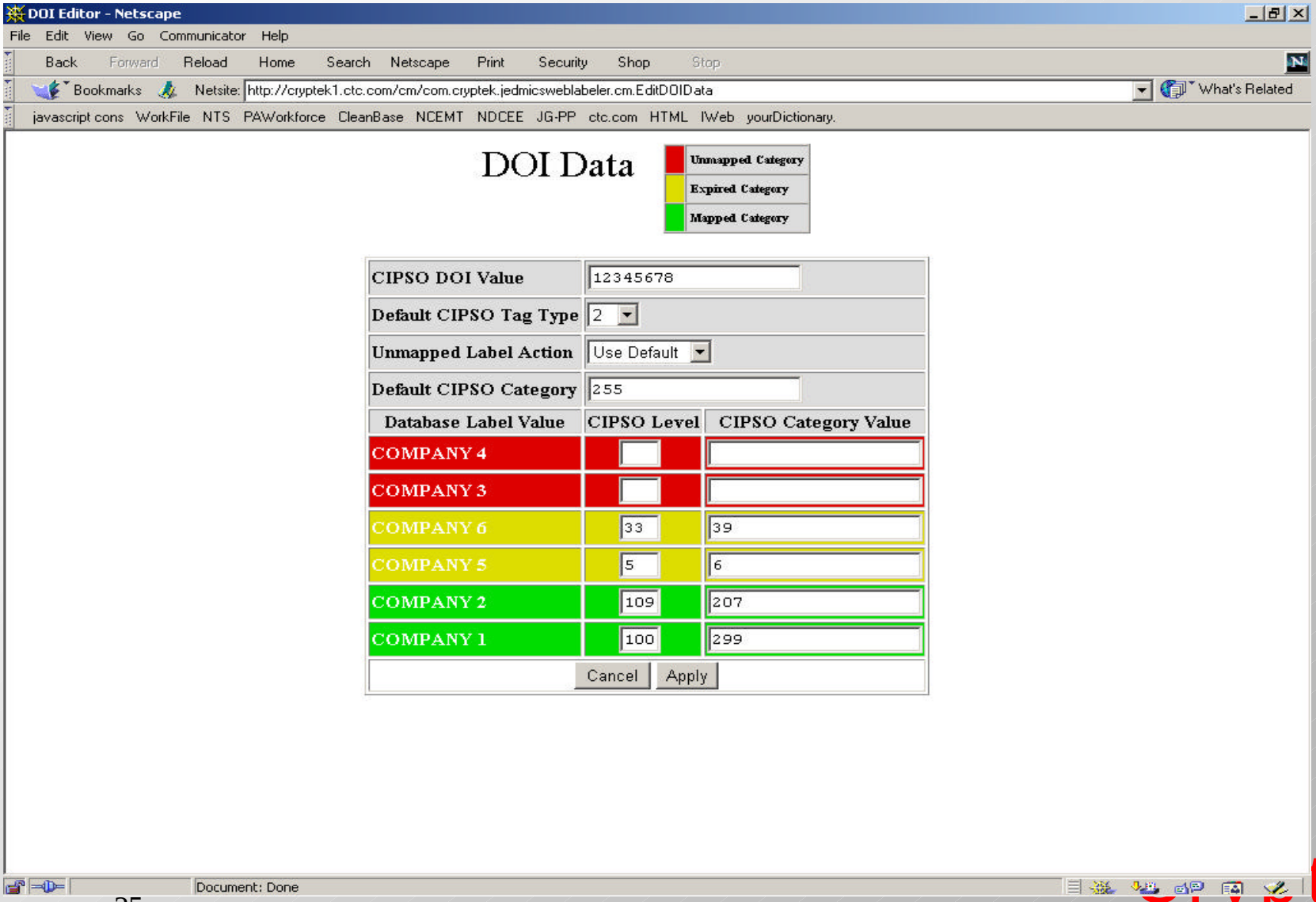
Cryptek®

Case Study – JEDMICS Release Policy Components

- User/Group
- Site/Location
- Data Owners
- Project related
- Rights
- CAGE Codes
- Federal Supply Codes
- Drawing Number
- Weapon Systems Code
- Distribution Statements
- Nuclear/Subsafe/etc
- Noforn

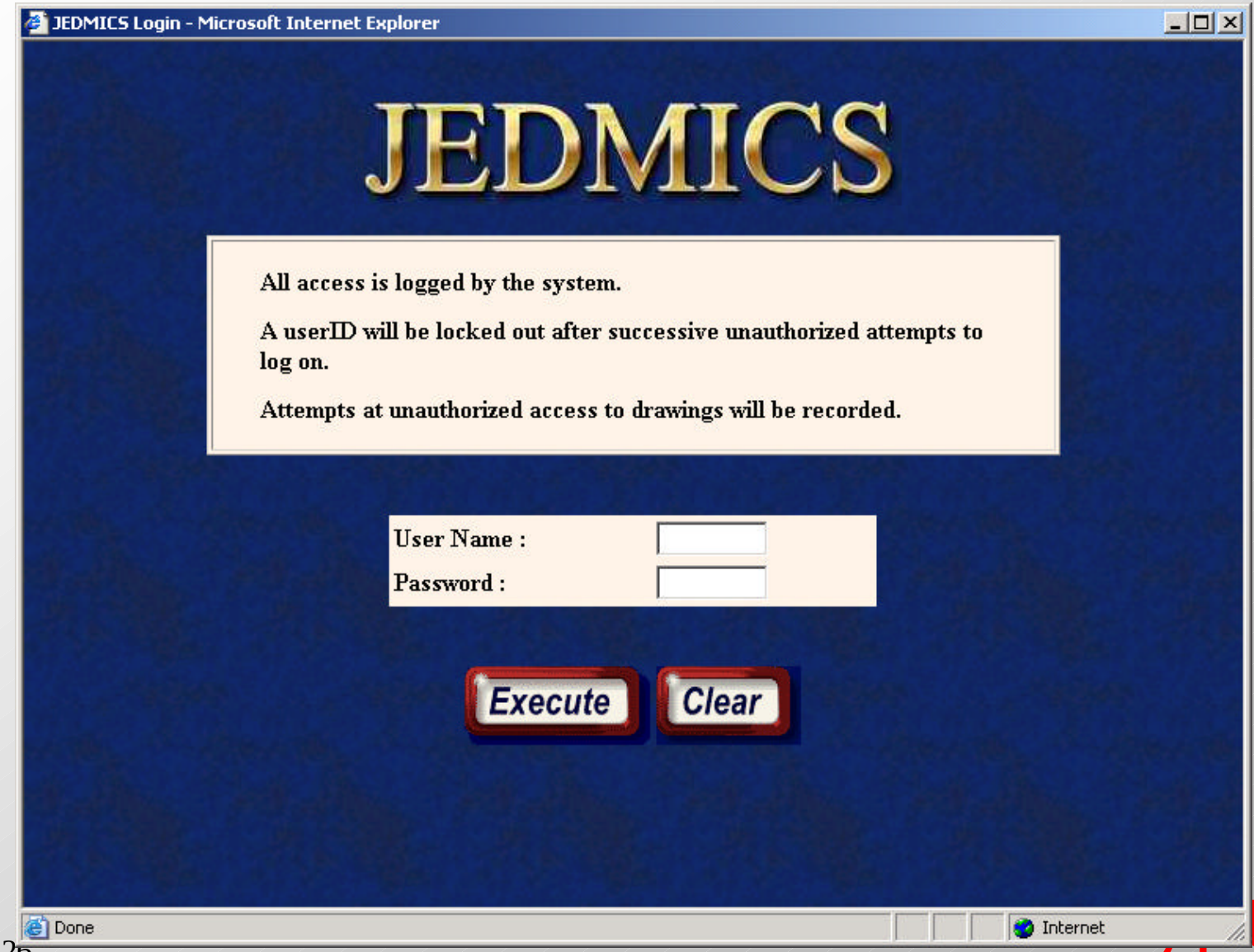
Cryptek®

DOI Editor

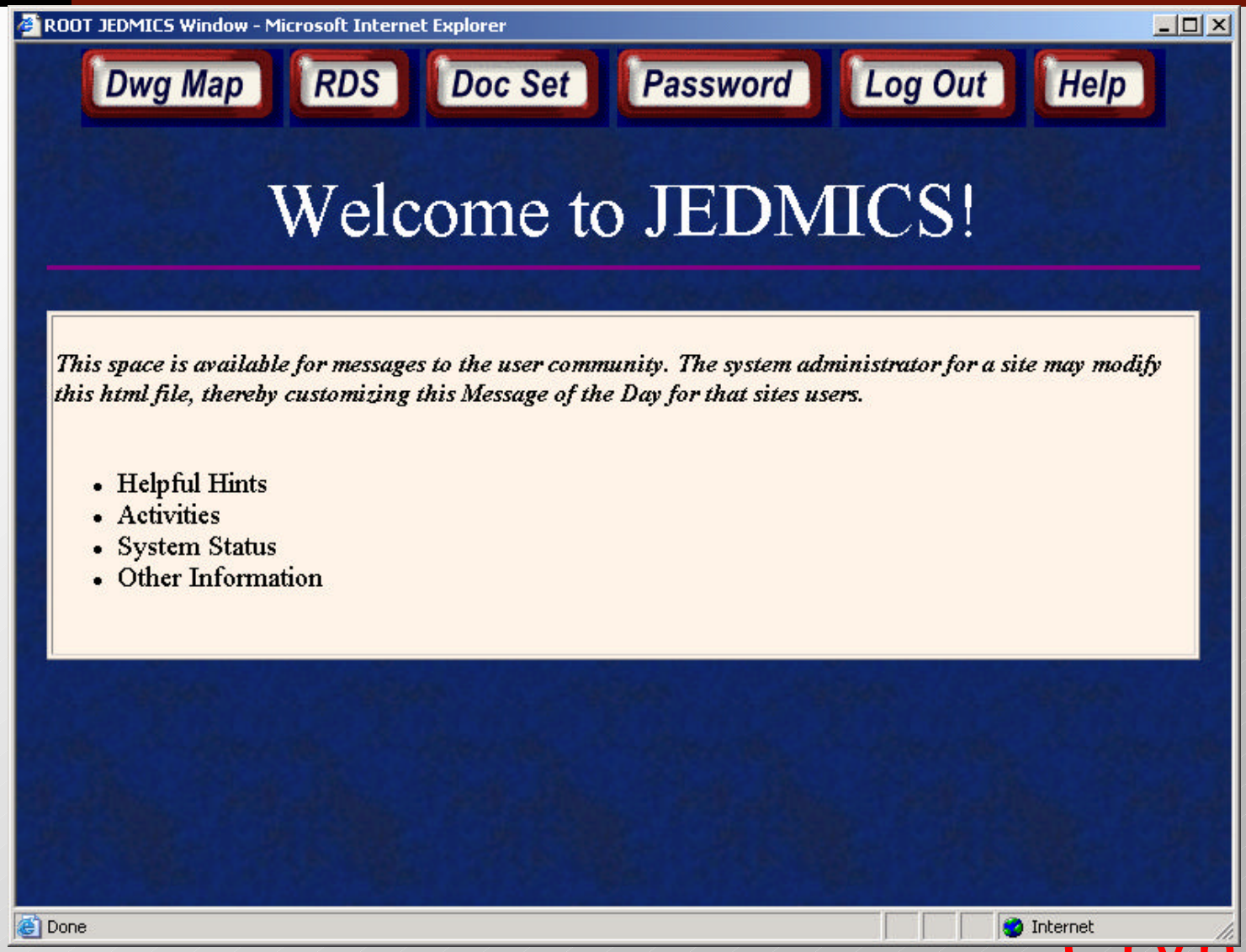


Cryptek®

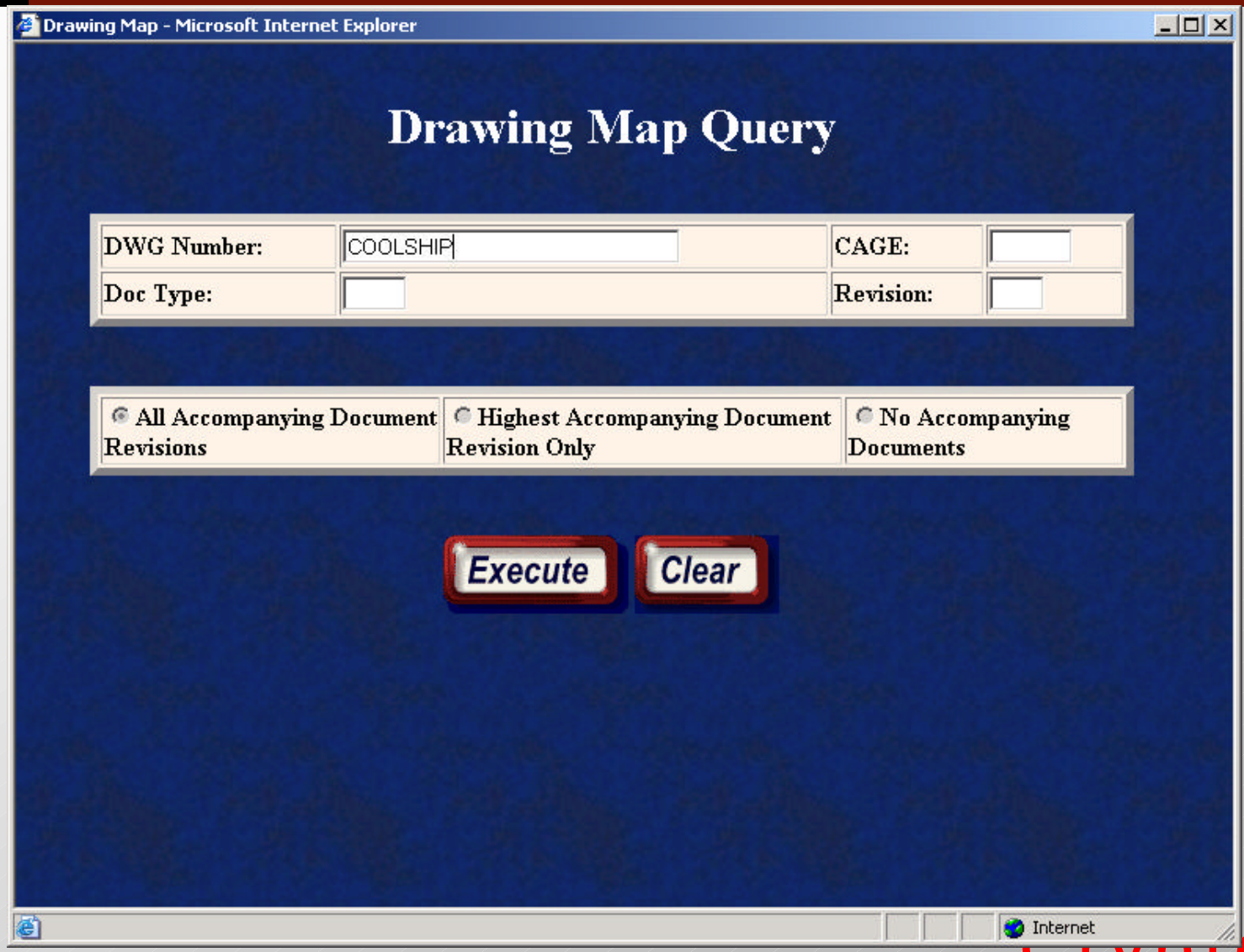
Log On Window



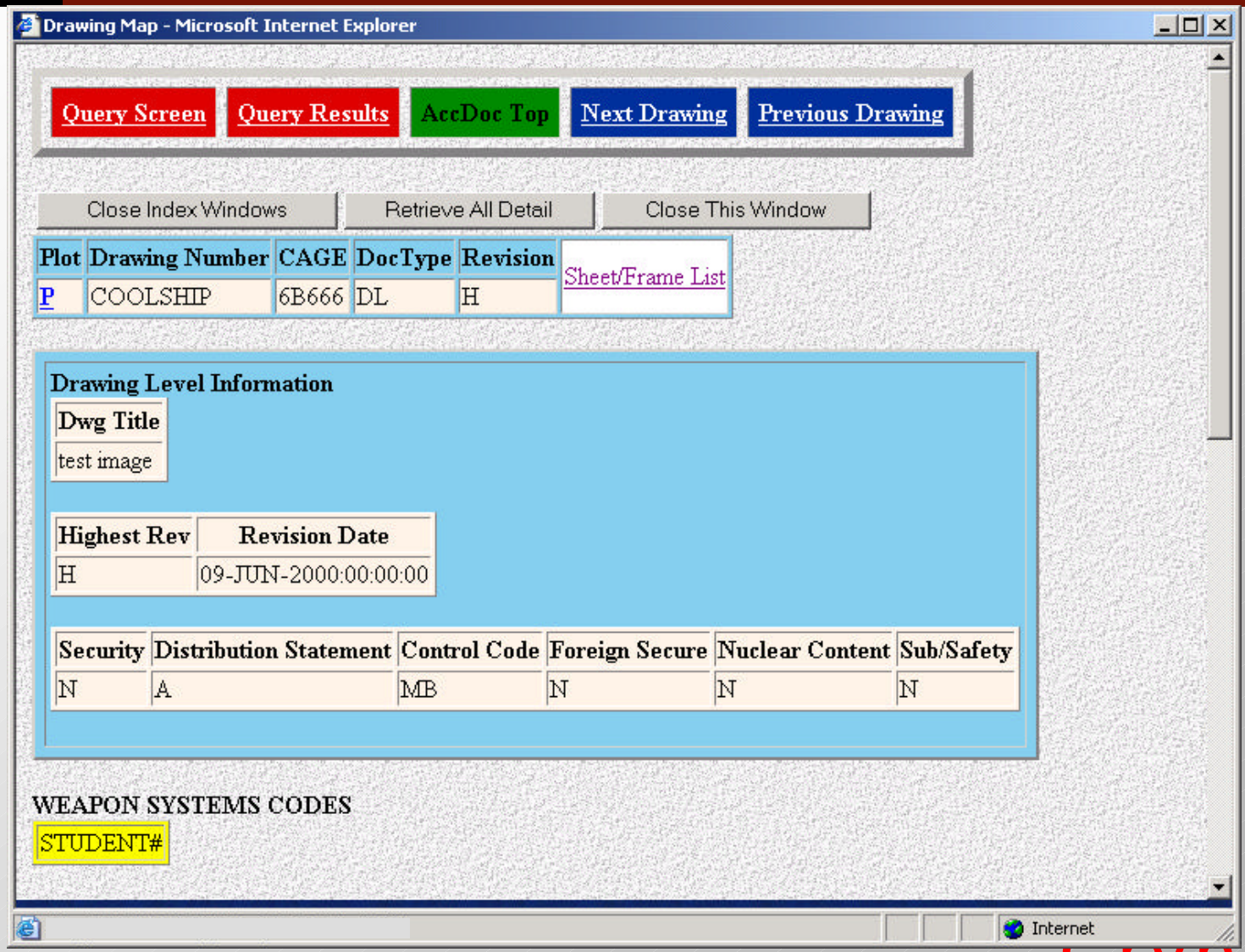
Root Window



Drawing Map Query Window

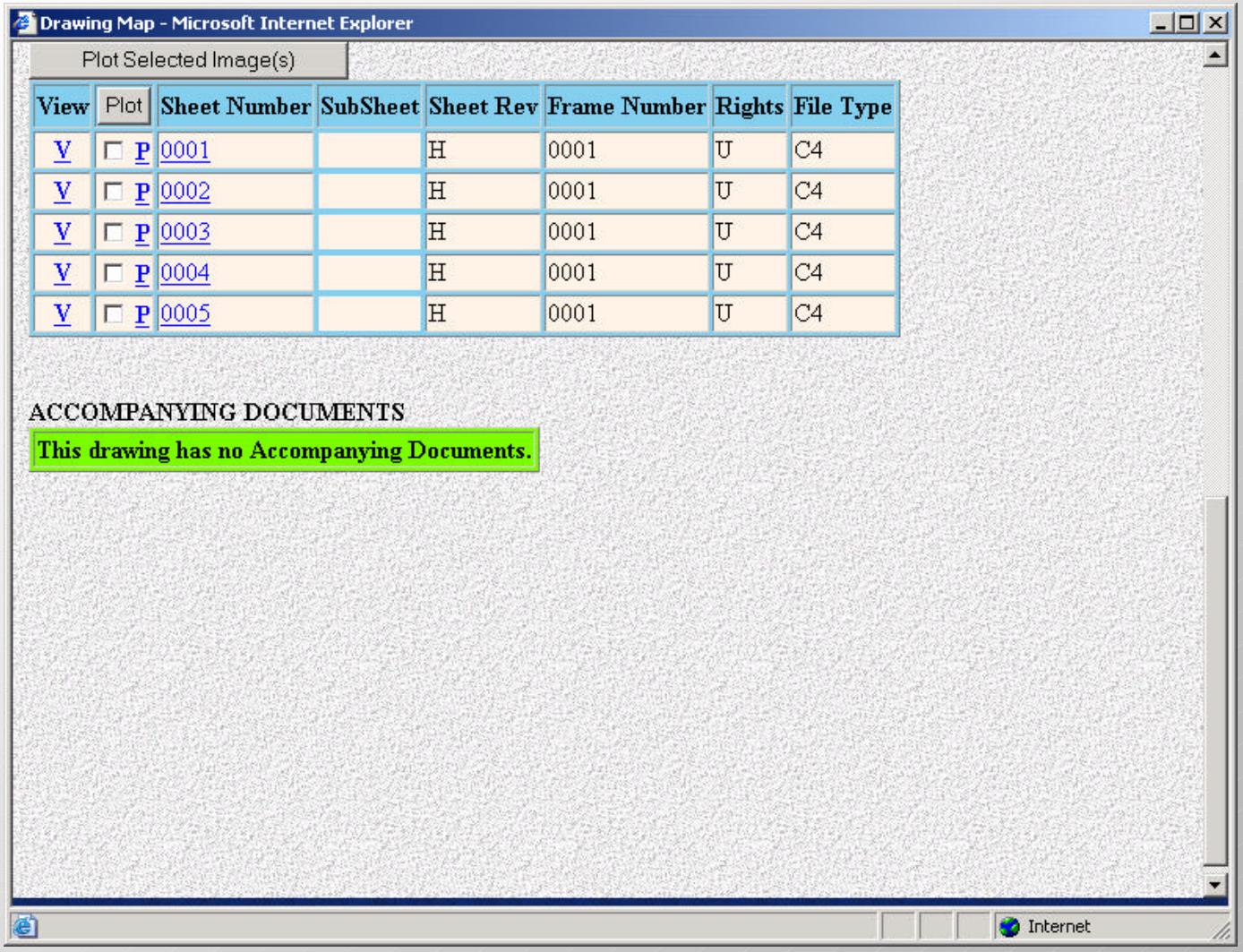


Drawing Map Detailed Information Window



Cryptek®

List of Drawings

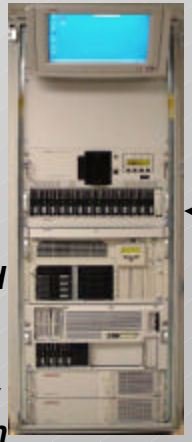


Cryptek®

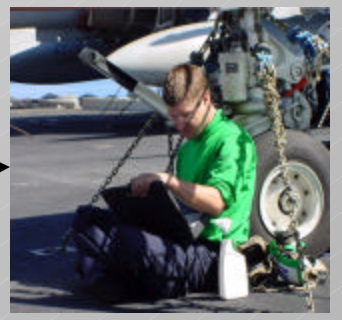
Joint AviationTechnical Data Integration

Package – Weapon System Web Sites
Deliver – Automatically download
Cache – local use/remote operations
Present – Integrated View of information

Managed Automated Delivery Of necessary information



Joint Knowledge Cache Server



Maintenance Technician Computers

Data Provider of Choice

Cryptek®

Designed for US and International Use

- Data Labeling integration to support release distribution of materials
- Cryptek Products provide mandatory enforcement mechanisms
- Software libraries implement labeling for stored objects
- Can also label by subnet, host, user, etc.

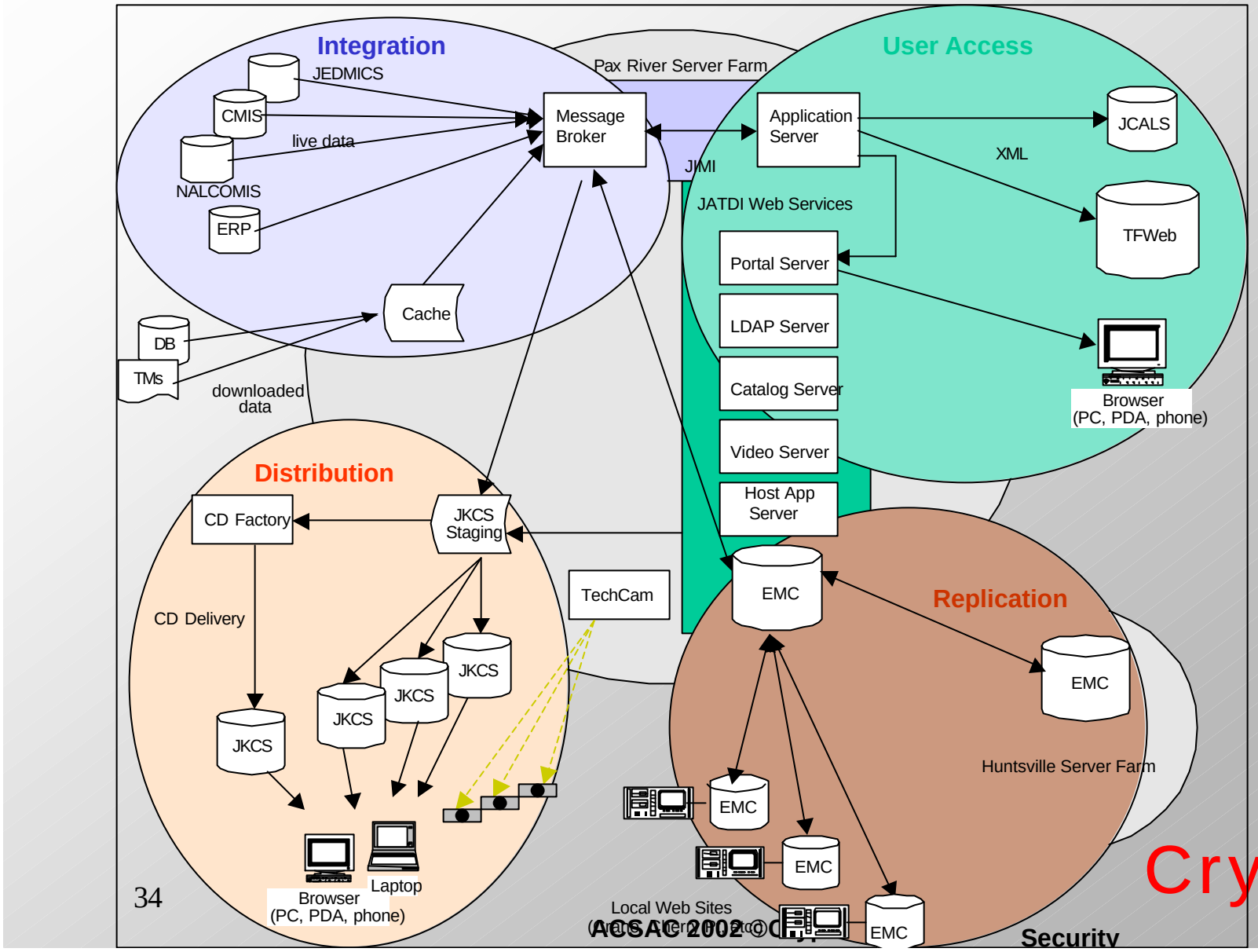
Cryptek®

JATDI Supports Many Data Types

- Documents
  - Office Documents (.doc, .xls, .pdf)
  - Engineering Data (.c4, .tiff, .pdf, ietms)
- Navigation Files
  - Web Pages (.htm .html, .shtml)
- Streaming Media
  - Audio Files
  - Video Files
- Applications
  - telnet, http, ftp, smtp
  - Legacy PC Applications via Citrix Metaframe

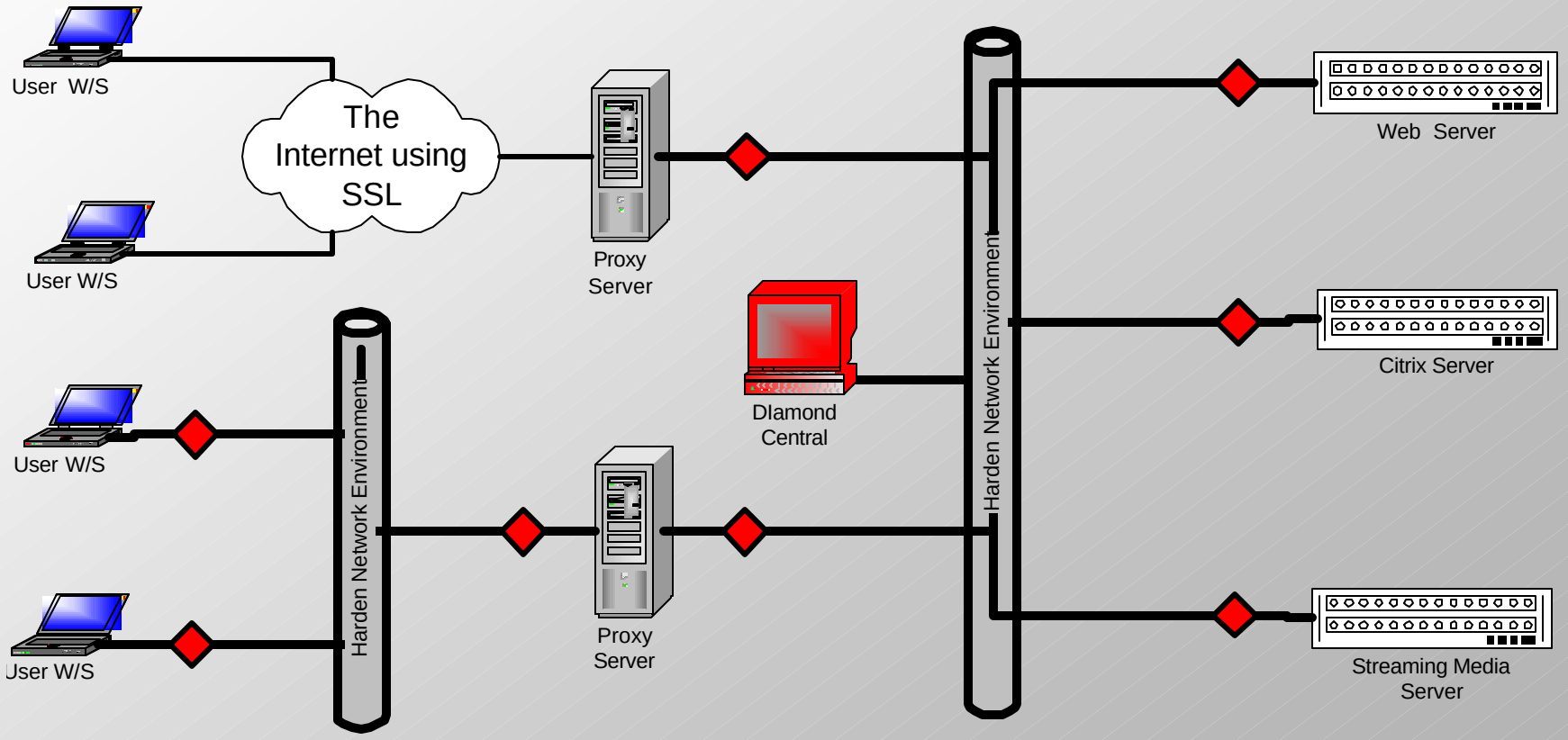
Cryptek®

JATDI System Architecture



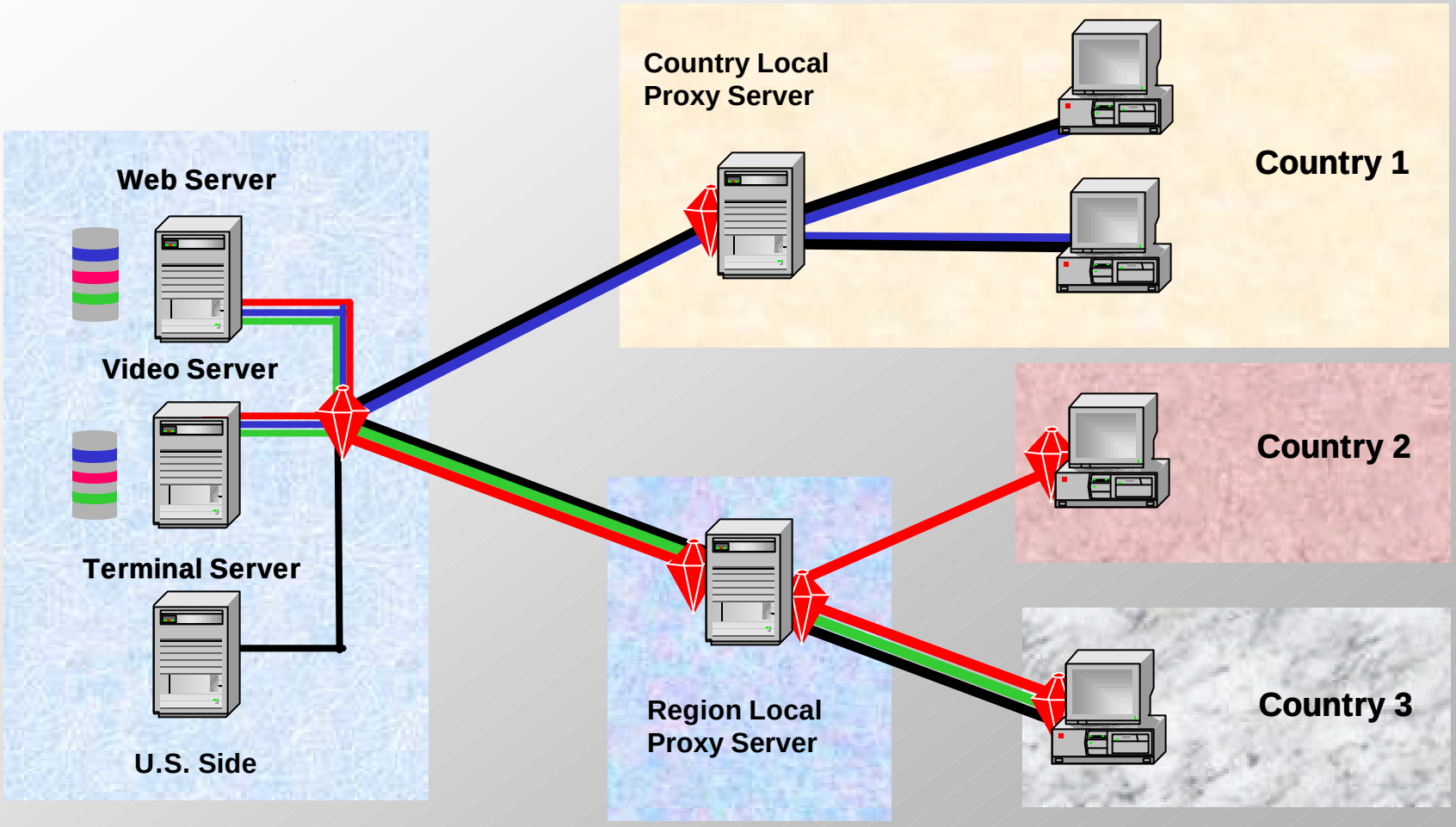
Cryptek®

Architecture



Cryptek®

FMS Network



Cryptek®

Cryptek Summary

- Cryptek's trusted access management system provides the highest level of protection available for information assets.
  - *Automatic* over-the-net secure upgrade
  - **Exportable to all but 7 hostile nations**
  - Diamond*TEK*'s trustworthiness is the result of years of trusted systems engineering experience, third party evaluations, and millions of dollars invested
  - Multiple certifications
    - FIPS 46, FIPS 140-1, FIPS 188,
    - Common Criteria at EAL 4 Completed
    - Works transparently with Type 1 Inline Network Encryptors.

Cryptek®

Backup Info Slides

Contact information:
Jack Wool
jwool@cryptek.com
jackwool@aol.com
978-697-1142

Cryptek, Inc.
1501 Moran Road
Sterling, VA 20166
571-434-2000
www.cryptek.com

Cryptek®

Cryptek Validated Products

Validated EAL4 DiamondTek product line is referenced on the NIAP web site:

www.niap.nist.gov/cc-scheme/ValidatedProducts.html

Listed in the categories for Firewalls, VPNs and Network Management. The detailed NIAP listing is located at:

www.niap.nist.gov/cc-scheme/cryptek-diamondtek.html

The detailed Validation report is located at:

www.niap.nist.gov/cc-scheme/CCEVS-VID4006-VR-02-0021.pdf

Cryptek®

Diamond*TEK* System Composition

The Diamond*TEK* system is a building block (security tool) for network designers to build secure network systems. The system is governed by a site-defined network security policy and comprised of the following components:

Diamond*CENTRAL*: the central security controller

Diamond*LINK*: an external drop-in network appliance comprised of a built-in firmware device and authentication card reader in a single external device

Diamond*PAK:* an external drop-in network appliance designed to protect specific servers on the network

Diamond*VPN*: an external drop-in appliance designed to protect the LAN or WAN network perimeter

Diamond*NIC*: a secure network interface card and authentication card reader

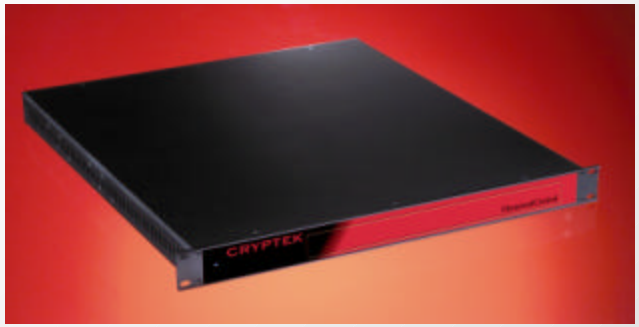
These components work together to create the secure network system on which host computers can communicate.

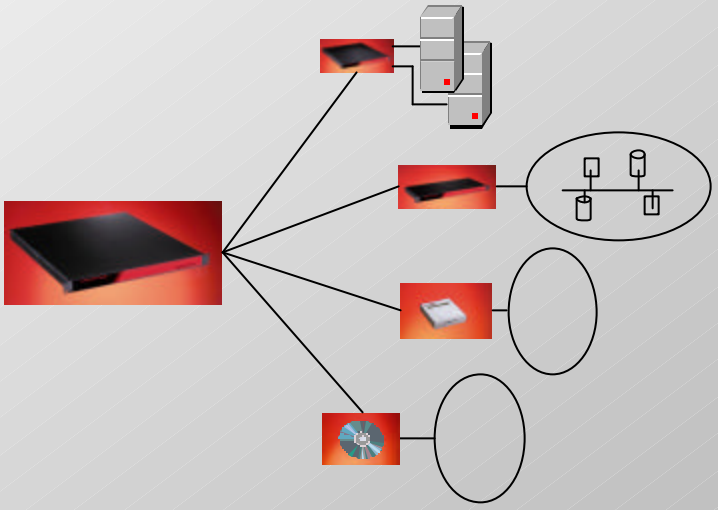
Cryptek®

Diamond*TEK* Distributed System Components

Cryptek®

System Components





- Diamond*Central*™
  - Central GUI controller for the Diamond*TEK* system
  - 1U rack mountable package
  - Provides central administration for network security
  - Communicates only with nodes it controls
  - Controls systems up to 5,000 nodes, 10,000 users
  - 140Mbps UDP, 110Mbps TCP 3DES throughput

Cryptek®