



Common Data Security Architecture (CDSA): A Potential Framework to Unify Information Assurance Approaches for the Warfighter

**A Briefing to The Open Group
Mobile Commerce 2000 London
11 April 2000**

**Russ Richards, Chief, Technical Architecture and Assessment Division
Center for Information Technology Standards (CFITS)
Defense Information Systems Agency/D6/JIEO
10701 Parkridge Boulevard
Reston, VA 20191-4357
Phone: (703) 735-3552 Fax: (703)735-3257 Email: richar1r@ncr.disa.mil**



General Requirements

- **For general purposes, DoD, like other users, wants universal security at little or no extra cost**
 - Sufficient or adequate level of security in purchased products
 - Standard component/feature at or for no additional charge
 - Secure for the DoD organizations as well as trading partners
- **From a design perspective, security in COTS products should be**
 - Designed in, not added as an afterthought
 - In background, checking its own integrity with no security holes
 - Extensible to allow for future needs to be easily incorporated
 - Capable of working essentially all computing platforms to meet normal conditions of network operations
 - Understood by programmers as the “standard way” to provide security



Perceptions Must Be Overcome to Meet Needs

- **Perceptions:**
 - Poor security of Internet (Intranets by association)
 - Internet has resulted in:
 - ◆ Multitudes of uncontrolled access to computer systems
 - ◆ Less control of IT facilities
- **Consequences (needs not being met):**
 - **eCommerce [and by extension mCommerce]:**
 - ◆ Reluctant and slow commitment by enterprises to migrate
 - ◆ Slow acceptance of, and use by, consumers
 - **Competing infrastructures that cause:**
 - ◆ Confusion
 - ◆ Expense
 - ◆ Delay
 - Legacy systems and migration are not accommodated
 - Innovation stifled due to competing, monolithic solutions



Security Policies Aided . . . Not Delivered . . . by IT Systems

- As a foundation, security policy must be well defined to cover physical, procedural, and technical issues.
- Technology alone cannot compensate for inadequate physical security, user error, or unexpected service failure.
- Procedural aspects are at least or just as important as technical issues.
- Main purposes of information security are to
 - **Maintain within IT systems:**
 - ◆ Availability
 - ◆ Integrity
 - ◆ Authentication
 - ◆ Confidentiality

} of

 - ▶ Data [Weakest element]
 - ▶ Programs
 - ▶ People
 - ▶ Services
 - **Correctly authorize and grant access controls to personnel involved with the system. [Authorization API + CDSA]**



Purpose of Security Is Not to Eliminate Annoyances but Espionage

- **Hackers and internal employees penetrating a system:**
 - Used to just annoy
 - Now majority are involved in purposeful espionage
- **Keeping a complex network up and running is very consuming (people, time, and money)**
 - Little time for risk assessment
 - Disaster recovery plans are not developed adequately and seldom tested and exercised
- **Emerging security technology will make security solutions easier to select and implement, such as:**
 - Digital signatures
 - Message authentication
 - Single sign-on
 - Cryptography (more practical and less costly)



Cryptography Is Involved in All Levels of Authentication

- Authentication is the first level of human/computer interface
- Authentication is based on:
 - **What the user *knows*** – lowest level: stored encrypted user name and password
 - **What the user *has*** – like ATM card added to what user *knows*, like PIN number in this case, provides medium security (of course, adding encryption of data transmitted from ATM terminal to bank).
 - **Who the user *is*** -- like biometric input (e.g. finger prints) contained in a smart card (what user has) will vastly improve authentication technology and provide higher levels.



Security Standards and the Need for a Common Security Architecture

- **Several data security and encryption standards exist**
- **Several standards cover cryptography, key management, and certificate management**
- **If they are to fit together and interoperate they need an architecture that**
 - **Comprehends and integrates them**
 - **Defines a common interface for both applications developers and security service providers**
- **CDSA is intended to serve those needs as an architecture framework based on:**
 - **Portable digital tokens**
 - **Digital certificates**



CDSA and Portable Digital Tokens

- **Portable digital tokens**
 - **Serve as a person's virtual persona for:**
 - ◆ **eCommerce [and by extension mCommerce]**
 - ◆ **Communications**
 - ◆ **Access control**
 - **These tokens are encryption modules, with some amount of encrypted storage.**
 - **They can be software or hardware depending on the application's security needs**
 - **They come in various forms and may have multiple functions aggregated into a single device, e.g. a digital wallet**



CDSA and Digital Certificates

- **Digital certificates**
 - Used to embody domain-specific trust.
 - Do not create any net trust models or relationships.
 - Are the digital form for current trust models.
 - ◆ A person may have a certificate for each trust relationship (such as multiple credit cards, checkbook, employer ID)
 - Are used for identity.
 - Can also carry authorization information. [potential overlap with Authorization API]



CDSA Adopters (Co-Travelers)*

A Significant Desirable Quality--Many Major Participants

Company in Alphabetic Order

	<i>CDSA-Related Product Type</i>
• Apple	Apple OSs, PowerTalk, KeyChain, and SSL v3 over CDSA
• Baltimore Technologies	PKI-Plus SDK
• Bull (France)	Developing a Linux CDSA Product
• Certicom	Elliptic curve Software, and Cryptographic Service Provider
• Compaq Computer	Digital Unix
• Chrysalis-ITS	Cryptographic Service Providers (Luna2. . .VPN hardware tokens & accelerators
• Cylink	CryptoKit toolkit, PrivateSafe SmartCard readers, PrivateCard SmartCards
• Entrust Technologies, Inc.	Specification Contributor
• Hewlett-Packard Company	HP-UX 11.0 (UNIX OS)
• IBM Corporation	IBM KeyWorks for AIX, Windows NT, OS/400 & OS 390 & several other products
• Information Security Corporation	Software Cryptographic Service Provider
• Intel Corporation	Creator of CDSA and reference implementation & LANDesk Management Suite
• Motorola	CipherNET SDK, CipherNET 1000, Registrar 2.0, & Certificate Authority Server 2.0
• RSA Data Security	RSA Certificate Security Suite
• Security Dynamics	SecurSight Enterprise Security Products
• Rainbow	Cryptographic Service Providers (CryptoSwift I & II Hardware Crypto Accelerators)
• Trusted Information Systems	Specification Contributor
• ValiCert	Trust Policy Service Provider (Certificate Validation Module for CDSA)
• Veridicom	Developing Fingerprint Reader, Biometric Service Providers for CDSA thru UAS

*Source: <<Richard Sargent, *CDSA Explained*, The Open Group, 1998, pp 88-90 (Bull added as The Open Group update.) >>



Independent Approaches*

Significant Drawback--Two Major Players Do Not Participate

Company

Alternative Approach

- **Microsoft Corporation**

Microsoft Crypto API

“One-point solution for secure communication across homogeneous networks (MS Windows and NT platforms). The Crypto API contains functions that allow applications to encrypt or digitally sign data, while providing protection for the user’s sensitive private key data. All crypto operations are performed by ancillary modules known as crypto service providers (CSPs). One CSP, the MS RSA Base Provider, is included with the MS operating system.”

- *MS CAPI Framework evolves under the discretion of Microsoft Corporation*
- *According to NSA, the current MS CAPI will run under the CDSA API*

- **Sun Microsystems**

SunScreen Secure Net/Java Crypto Arch

“This is a versatile network security system for access control, authentication, and network data encryption. It is the latest release of proven network security products from Sun, integrating SunScreen Secure Net, SunScreen™ SKIP, and SunScreen™ SPF-200. SunScreen Secure Net can divide a network into discrete areas, each served by an interface that provides customized fine-grain access control. Using filtering rules, SunScreen Secure Net controls the access from one area of a network to another, as well as access to the Internet or other external networks. SunScreen Secure Net consists of a rules-based, dynamic packet-filtering engine for network access control, and an encryption and authentication engine that enables the creation of secure virtual private network (VPN) gateways by integrating public-key encryption technology. It

is administered through an easy-to-use graphical user interface (GUI) via a secure Web browser connection.”

- *SSCN/JCA evolve under the discretion of Sun Microsystems*
- *DoD is investigating if current SSSNet will run under the CDSA API*

*Source: <<Richard Sargent, *CDSA Explained*, The Open Group, 1998, pp. 18-19 >> and
<<<http://www.sun.com/software/white-papers/wp-security-securenettech/#2ai>>>



DoD/DISA General Security Requirements*

- **What is needed in DISA Common Operating Environment (COE) applications**
 - **Accountability (identification and authentication, audit)**
 - **Confidentiality (access control, encryption)**
 - **Integrity (cryptographic hash, access control)**
- **Where is it needed**
 - **Per link**
 - **End to end**
 - **In place**
 - **Multicast**

*Source: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



DoD/DISA Requirements*

- **Security service requirements depend on the organization's responsibility to the system:**
 - **Development**
 - **Management**
 - **System integration**
 - **Accreditation**
- **Development organization requirements:**
 - **Can be used to add security services to new and existing applications**
 - **Provides needed security services**
 - **Is easy to use**
 - **Requires minimum changes to code (independent of the specific implementation used)**

*Source: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



DoD/DISA Requirements*

- **Management organization requirements:**
 - Is modular; installs only what is needed
 - Can evolve as technologies change
 - Is interoperable across platforms and products
 - Can expect future support from vendor
- **System integration organization requirements:**
 - Can combine solutions provided by disparate vendors into single system
 - Can apply management-defined policies to applications from different developers
- **Accreditation organization requirements:**
 - Provides all appropriate security services
 - Meets robustness requirements

*Source: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



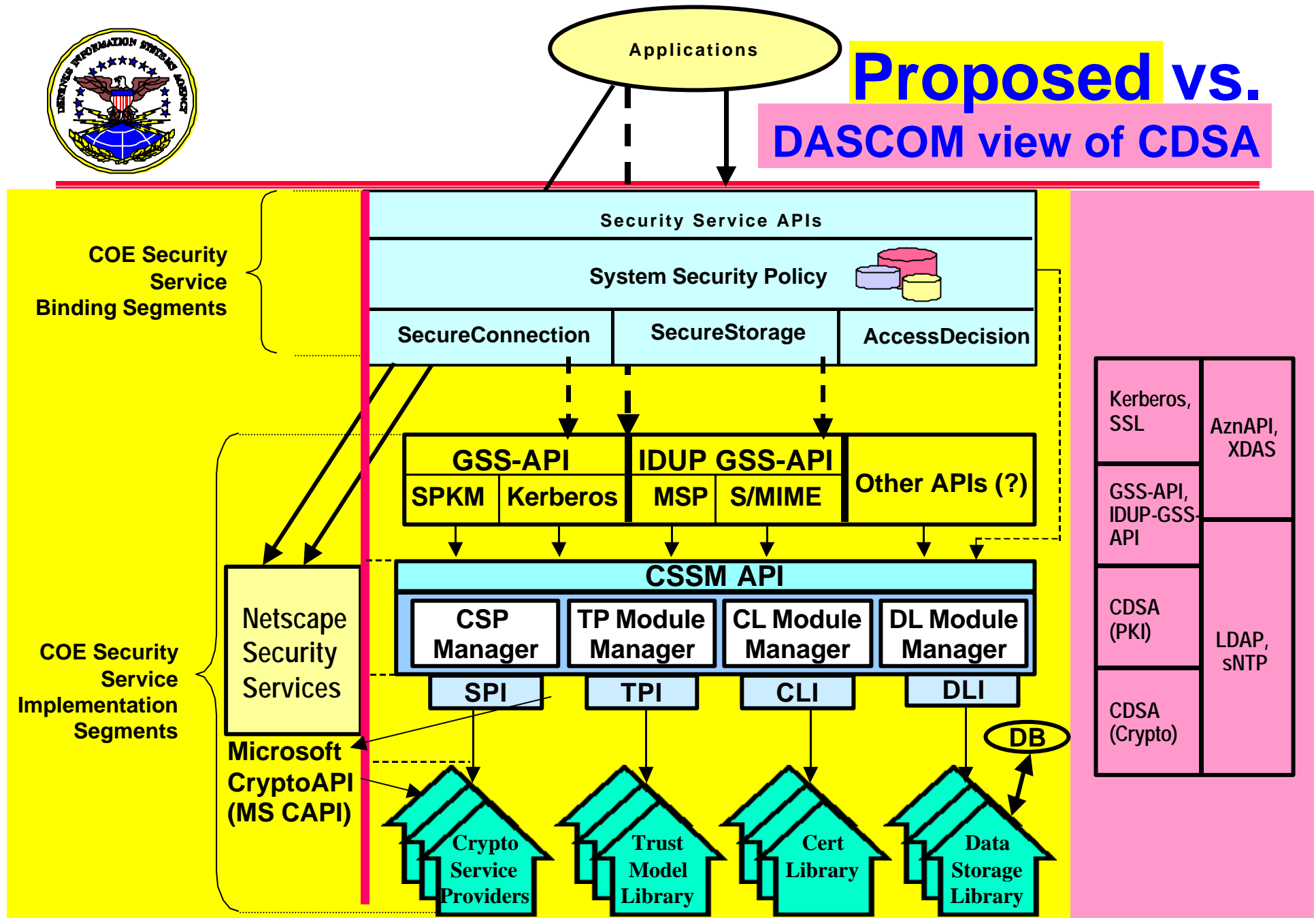
DoD/DISA Requirements*

- **Discussions with DISA application developers (e.g. COP and GCSS) indicate:**
 - They need a secure connection capability
 - That looks like existing unsecured socket calls
- **This means:**
 - Using sockets is a familiar approach
 - Developers want security to be transparent and NOT require specific actions on their part
 - Developers indicated they could develop “wrappers” for detailed interfaces (such as GSS-API), but this would be more complex and difficult to maintain
 - If industry (or government if necessary) provides a single security architecture API -- a solution which closely matches existing socket connection -- it would be welcome and reduce overall maintenance

*Source: Amgad Fayad (afayad@mitre.org), “DII COE Security Services Architecture Framework (SSAF),” unpublished presentation to The Open Group, Feb 2000.



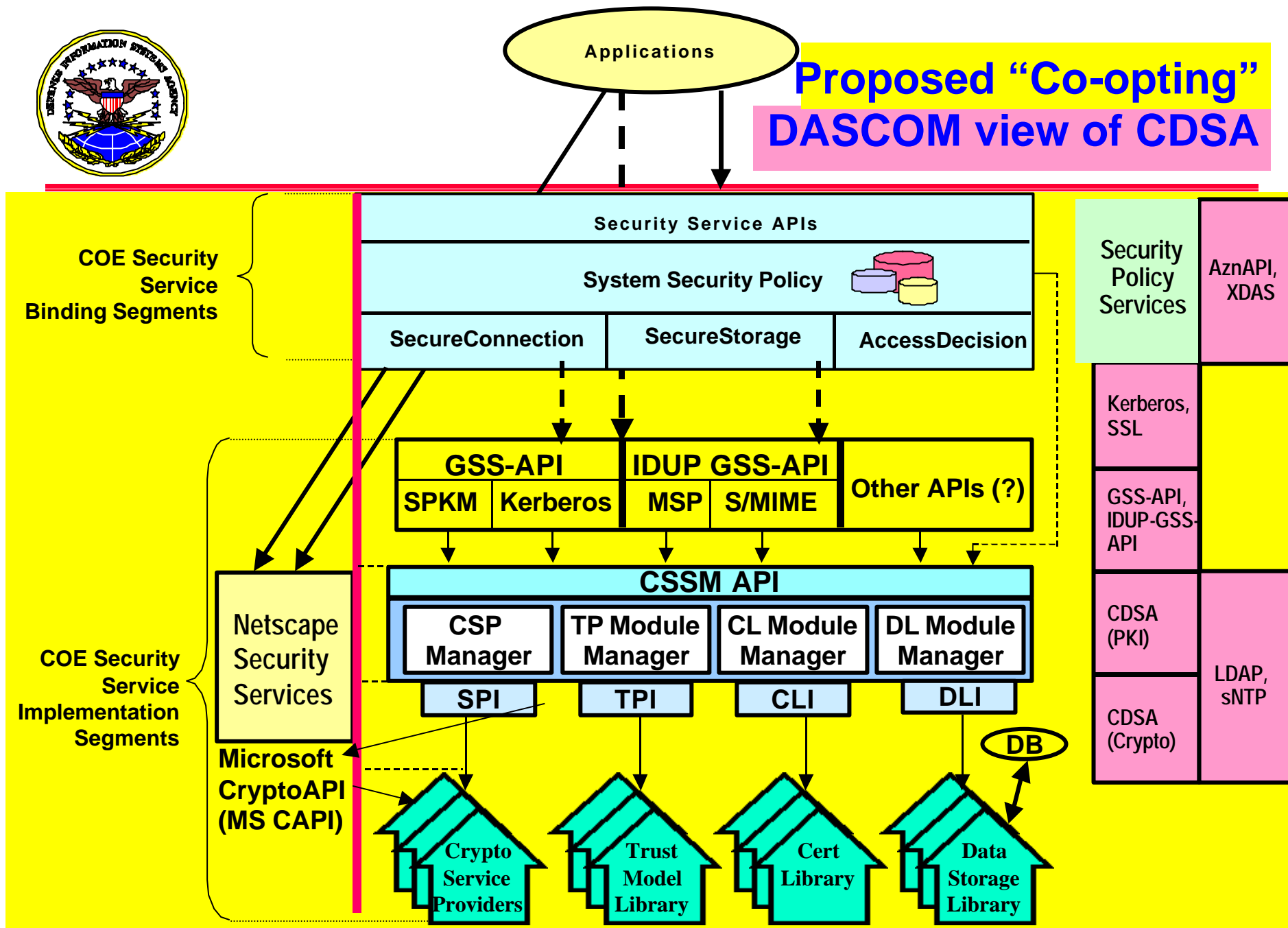
Proposed vs. DASCOM view of CDSA



*Source: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



Proposed "Co-opting" DASCOM view of CDSA

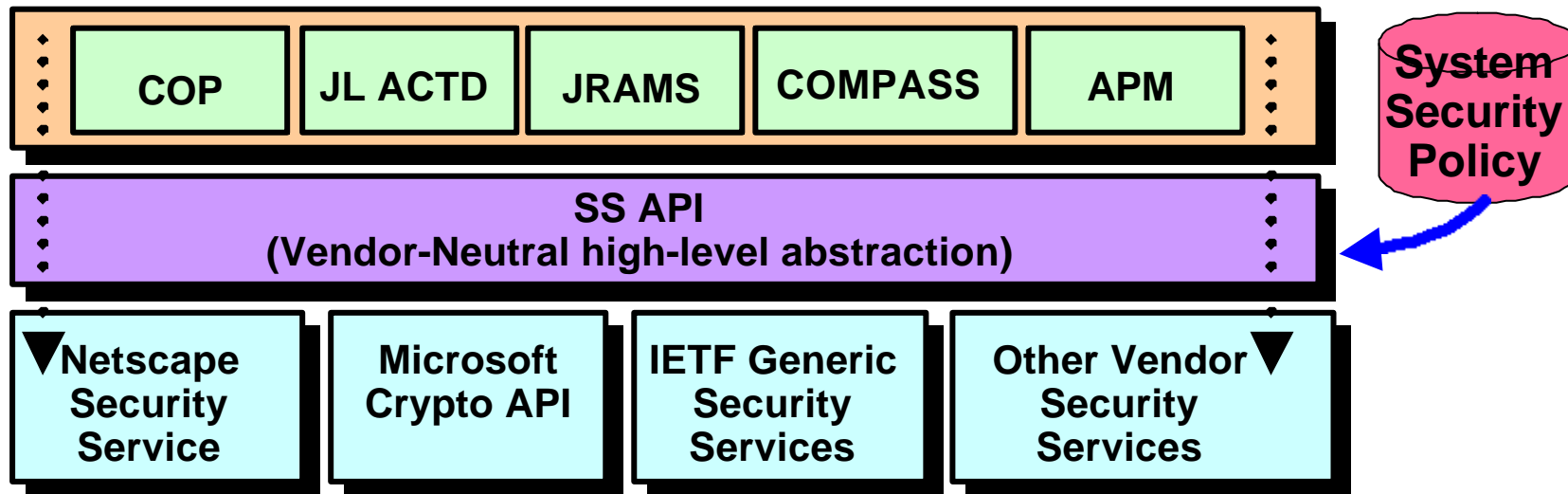


*Source: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



DoD May Need High Level API(s) (not currently offered in CDSA)

- In DoD, Security Services are needed for heterogeneous platforms:
 - Microsoft NT®
 - UNIX® (e.g., Sun, HP, Compaq, etc.)
 - Linux (e.g., Red Hat, Cadre)
 - Real-time embedded OSs (e.g. Lynx, VS-Works, QNX)



Note: Red = DII COE reference platforms

*Source: Modified from: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



Security Products and Standards

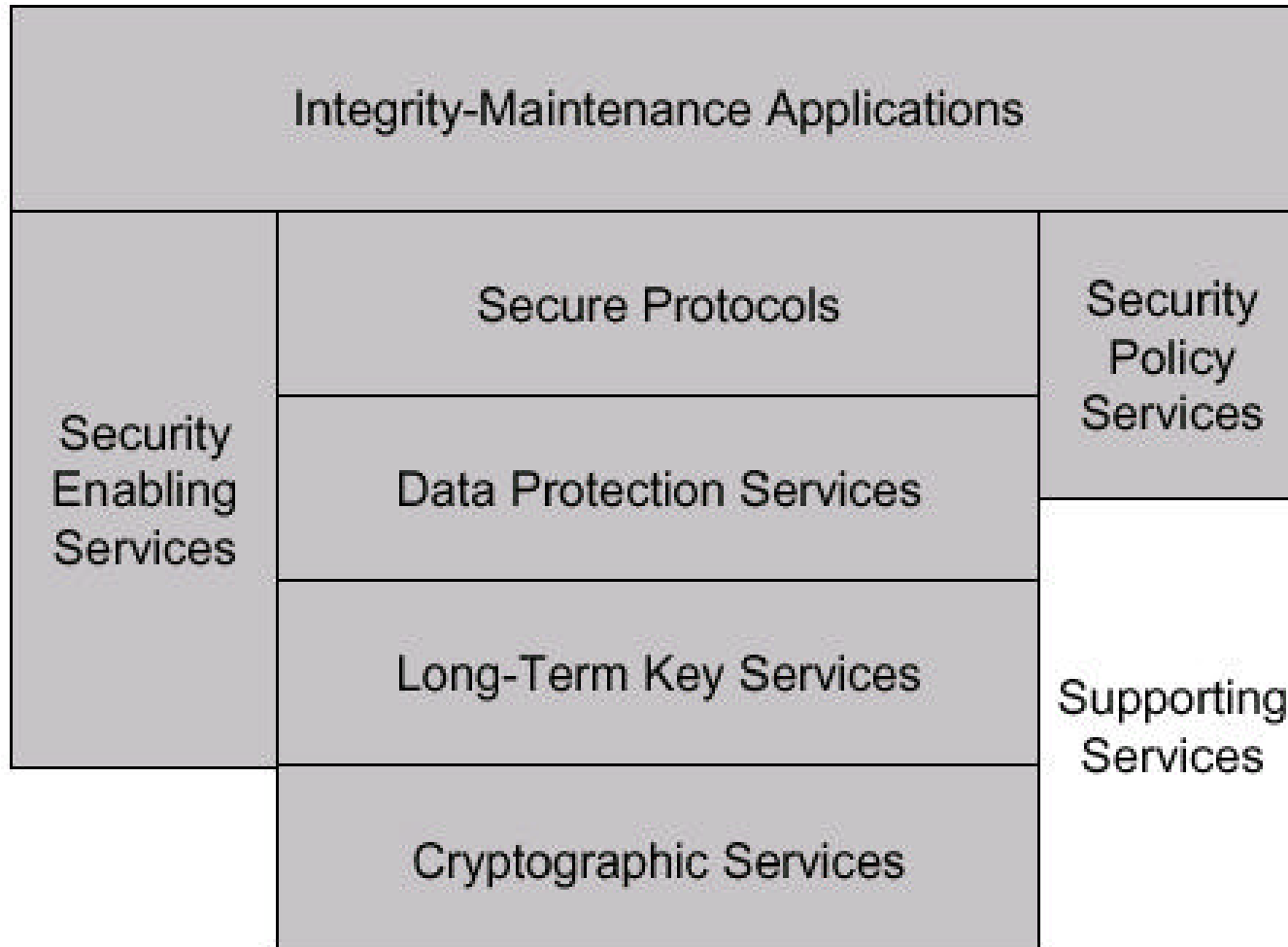
(ala Dr. Robert Blakley)

Firewall, AntiVirus, Intrusion Detection		
XSSO, Security Context Mgmt	Kerberos, SSL	aznAPI, XDAS
	GSS-API, IDUP-GSS-API	
	CDSA (PKI)	LDAP, sNTP
	CDSA (Crypto)	



Secure Systems Architecture

(ala Dr. Robert Blakley)





Summary: Benefits of a High Level API

- Provides high-level socket-like secure connections
- Provides applications with system security policy
 - Consistent system security policy within a system
 - Applications do not have to change with policy changes
- Provides a thin isolation layer between a security product and COE applications for portability
- Removes control of some communications channel characteristics from application programmer
- Provides secure communication by default using system security policy
 - Requires minimal application programmer awareness
 - Reduces security vulnerabilities



Future Directions

- **If Government API proves successful for alternative solution products, offer the API to The Open Group as a high-level API for CDSA**
- **Develop SS API versions**
 - **To provide security to issues beyond the current SS API approach which is limited to point-to-point communication**
 - **To address a wider range of problems:**
 - ◆ **Digital signatures**
 - ◆ **Accountability, integrity, and confidentiality**
 - **End to end**
 - **In place**
 - **Multicast**
- **Encourage The Open Group to adopt Authentication API in CDSA**

*Source: Modified from: Amgad Fayad (afayad@mitre.org), "DII COE Security Services Architecture Framework (SSAF)," unpublished presentation to The Open Group, Feb 2000.



CFITS PKI Work

- **CFITS has been analyzing commercial PKI standards versus DOD requirements and COTS products**
- **Role of CFITS is to assist in choosing commercial standards approaches to PKI requirements for DoD**
- **CFITS will be joining PKI Forum to achieve standards goals**
- **CFITS JTA (security section) includes C/S/A agreed-to PKI standards**
- **PKI documents found**
 - www-pki.itsi.disa.mil
 - www-jta.itsi.disa.mil (Section 2.6, Security Systems)