DSSeries Security

Network Computing,
Public Key Infrastructure,
and the Enterprise

Bob Blakley

IBM Lead Security Architect

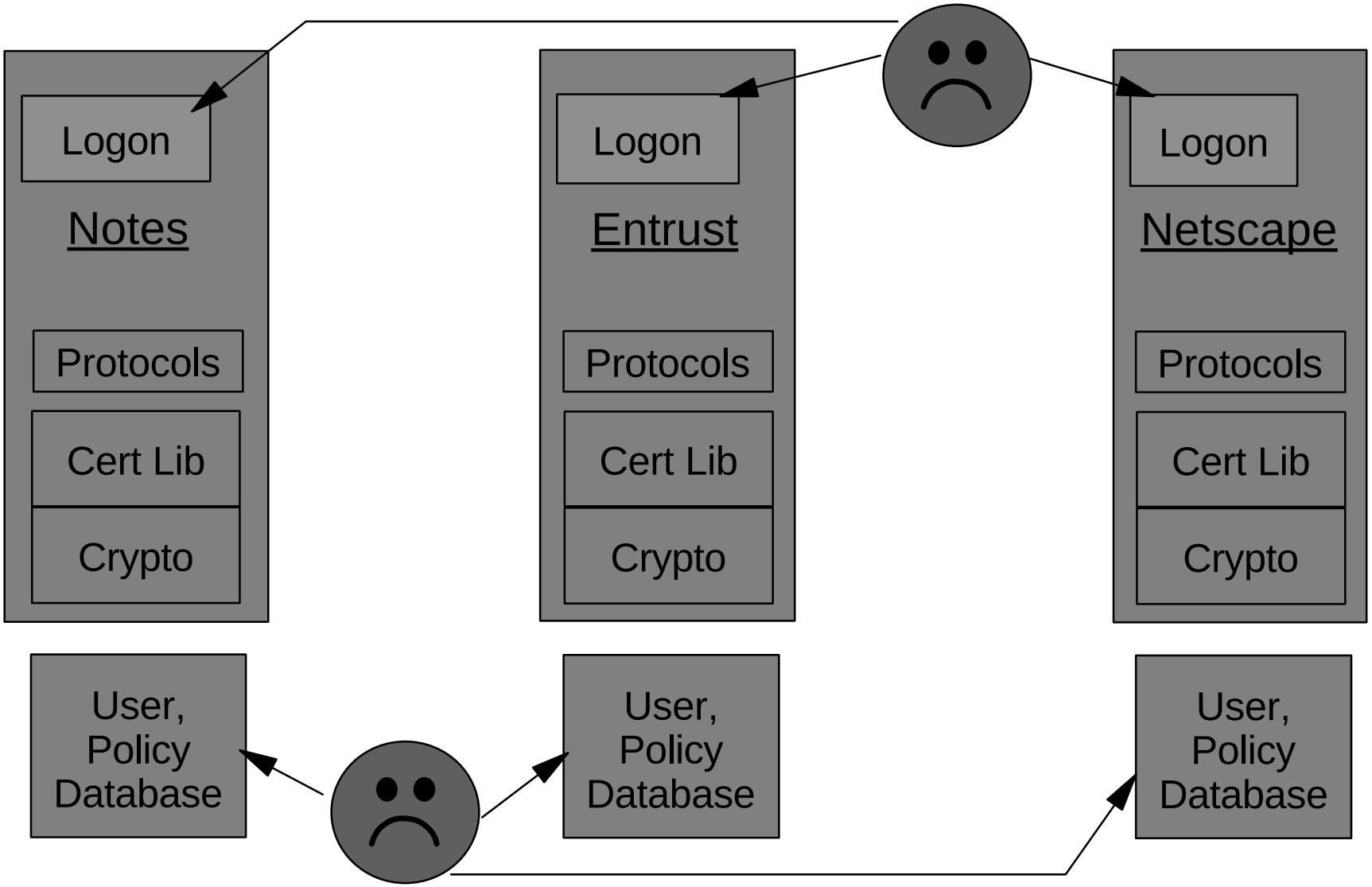
blakley@us.ibm.com

ARCHITECH
IT EXECUTIVE CONFERENCE

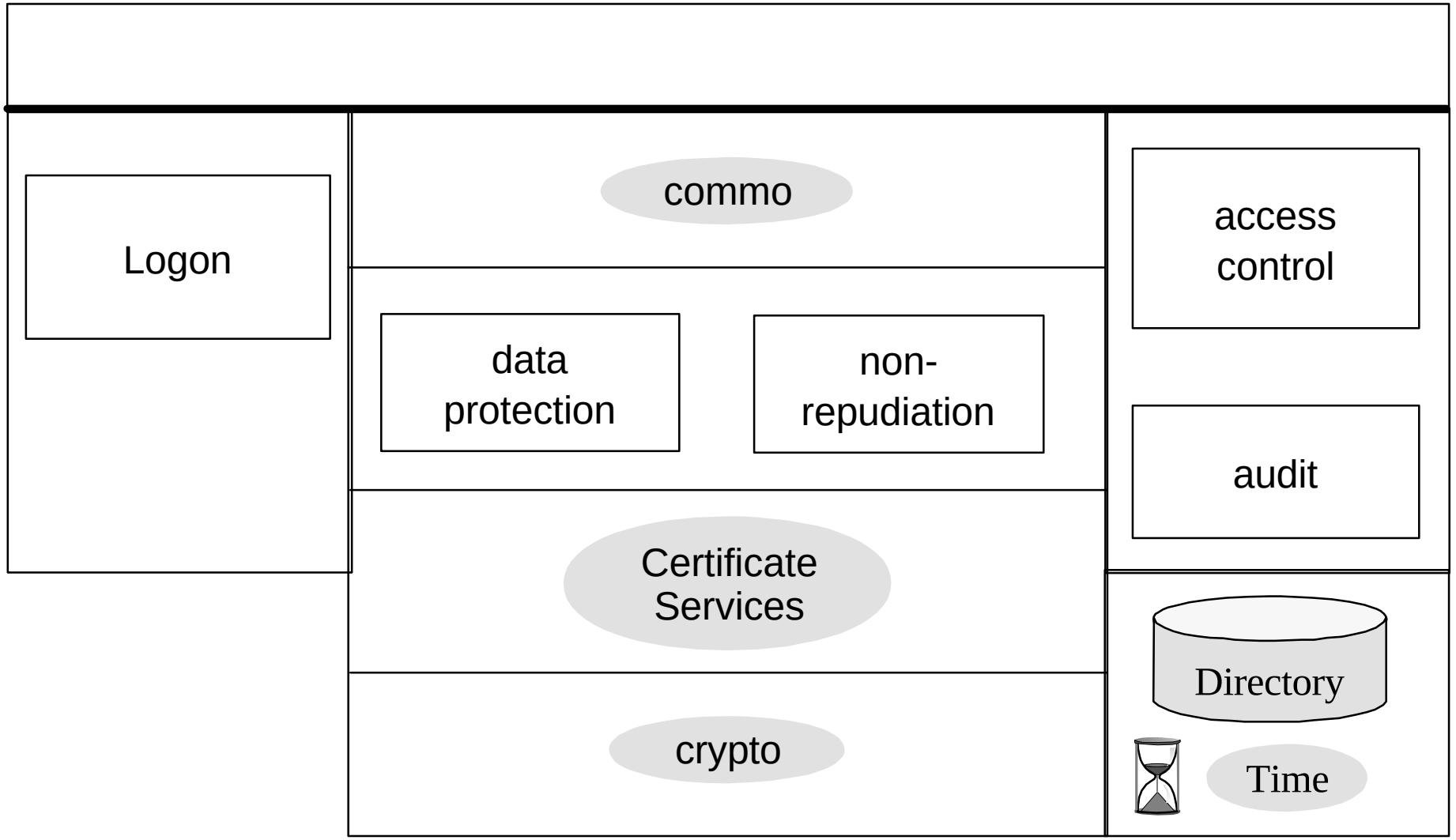
What is Security?

Requirement	Function	Technology
Authorization	Data Protection	Key Distribution
		Origin Authentication
		Data Privacy
		Data Integrity
	Access Control	Policy Enforcement
		Privilege Management
		User Authentication
Accountability	Audit	
		Event Generation/Disposition
	Non-Repudiation	Data Signature
		Trusted Time
Availability	Service Continuity	Replication
		Resource Quotas
		Rate Limitation
	Disaster Recovery	Data Backup / Restore
		Key Recovery
Assurance	Engineering Practice	Design / Test / Verify
	Development Process	Documentation
	Operations Management	Integrity Maintenance & Restoration
Administration	System Configuration	Install / Configuration / TCB Mgmt.
	Mechanism Management	Activation / Defaults
	Policy Management	User, Authorization, Audit, Trust, ...

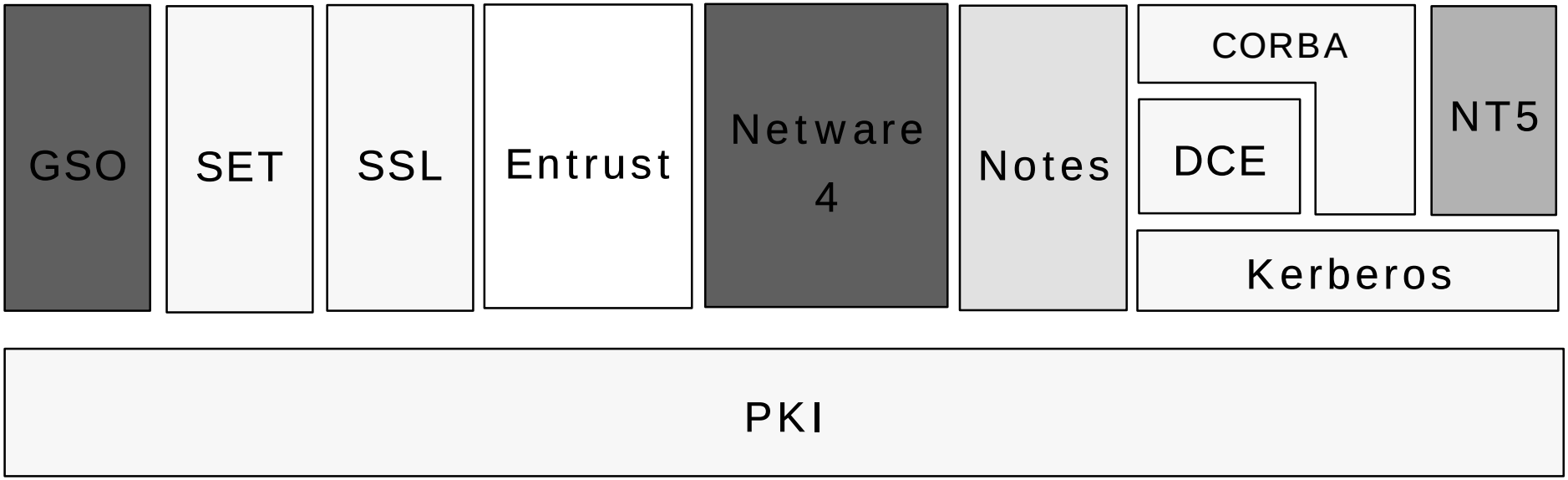
Why a PKI?


Logon
Notes
Protocols
Cert Lib
Crypto
Logon
Entrust
Protocols
Cert Lib
Crypto
Logon
Netscape
Protocols
Cert Lib
Crypto
User, Policy Database
User, Policy Database
User, Policy Database

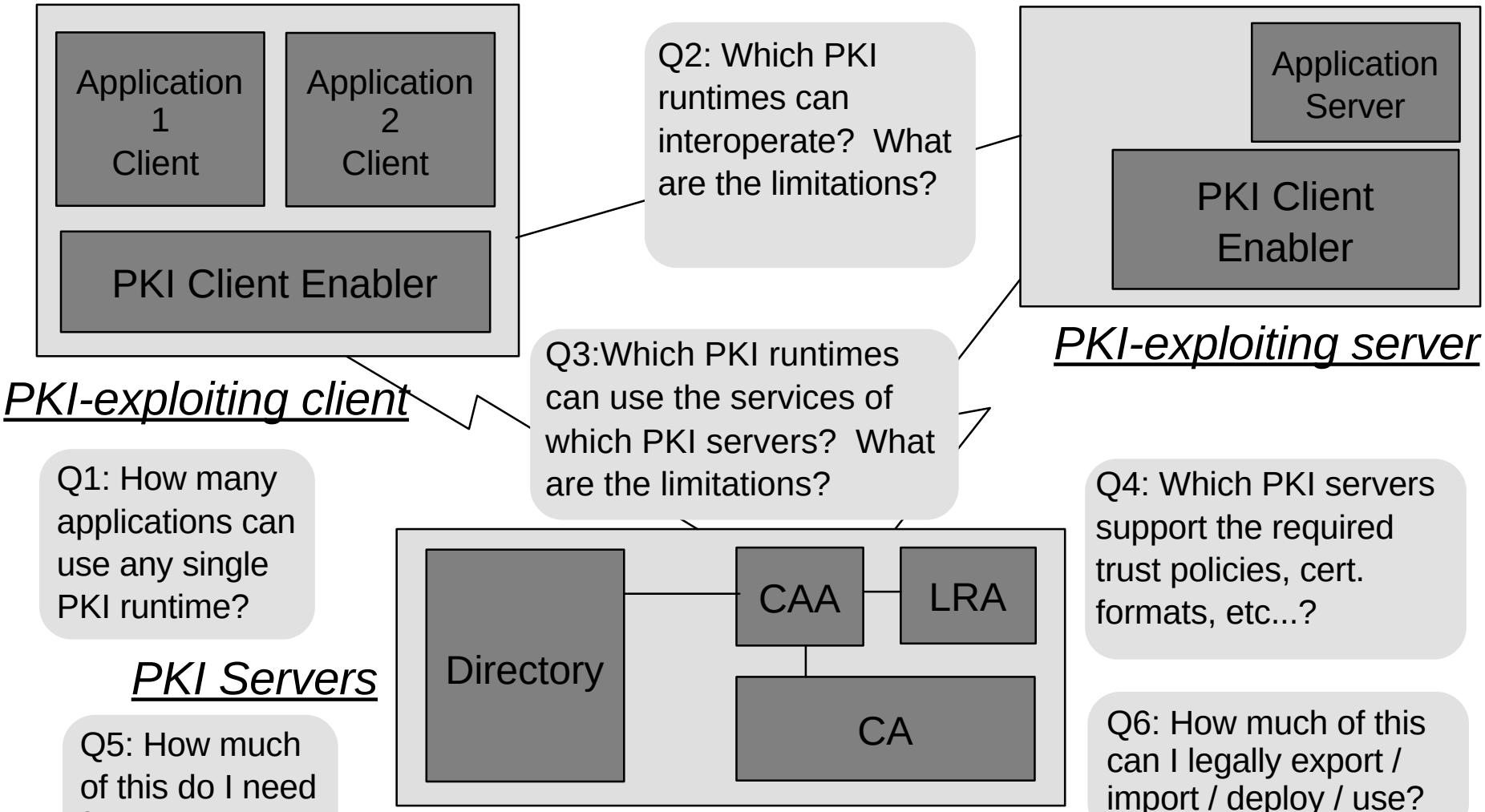
What's in the PKI?



PKI - The Integrating Foundation



Why PKI Standards?



What Kinds of PKI Standards?

- Formats & Protocols
  - ► enable multivendor interoperability
- Programming Interfaces
  - ► enable application portability
  - ► reduce development cost
- Programming Interfaces *and* Formats & Protocols
  - ► enable implementation replaceability
  - ► runtime replaceability requires Frameworks
- Profiles
  - ► to tailor flexible infrastructure to specific needs

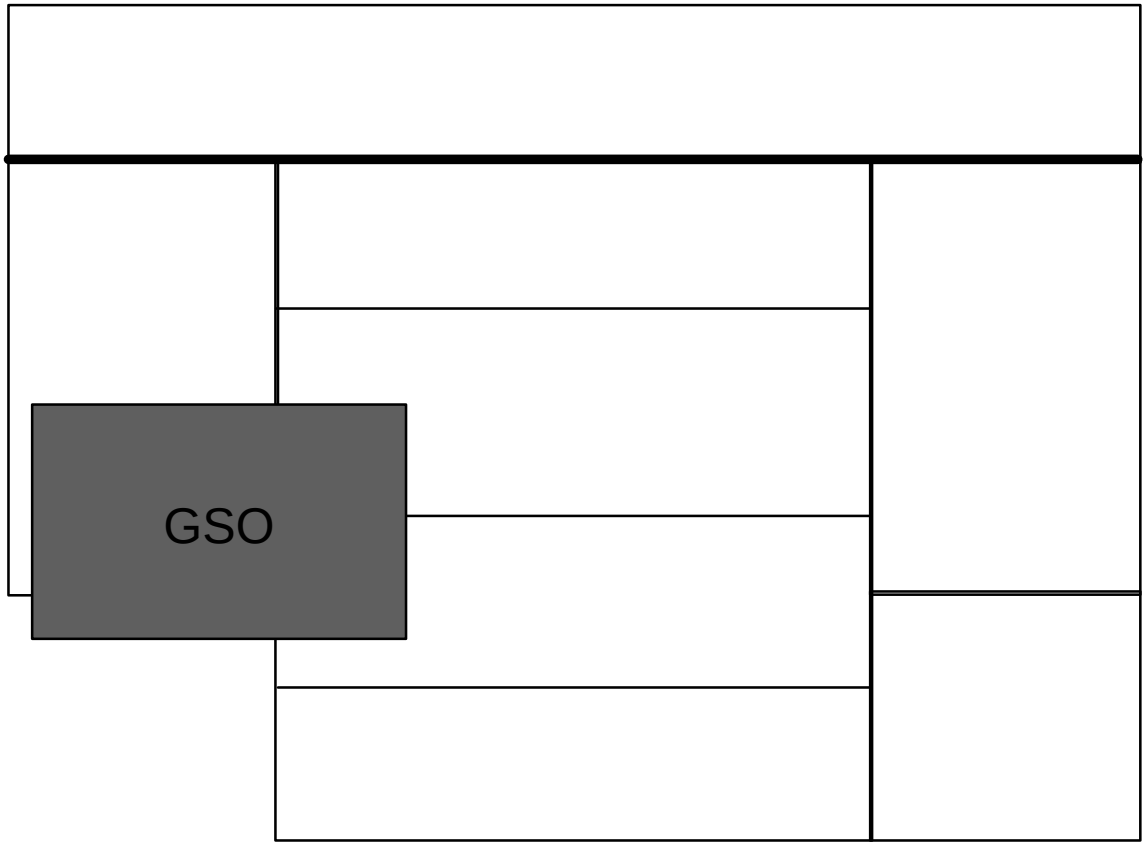
Which PKI Standards?

- Formats & Protocols
  - X.509 v3 Cert. format, X.509 v2 CRL format
  - PKIX Certificate Management Protocols
  - LDAP Directory Access Protocol
  - SSL v3 Secure Communications Protocol
  - IETF Security Multipart Protocol
  - RSA PKCS 7, PKCS 10, PKCS 12 formats
- Programming Interfaces
  - CDSA CSSM Crypto, Cert Management, optional Key Recovery APIs
  - PCSC Smartcard APIs
  - Open Group XSSO APIs
  - IETF GSS-API, IDUP Data Protection APIs
  - OMG CORBAsecurity
  - Java security

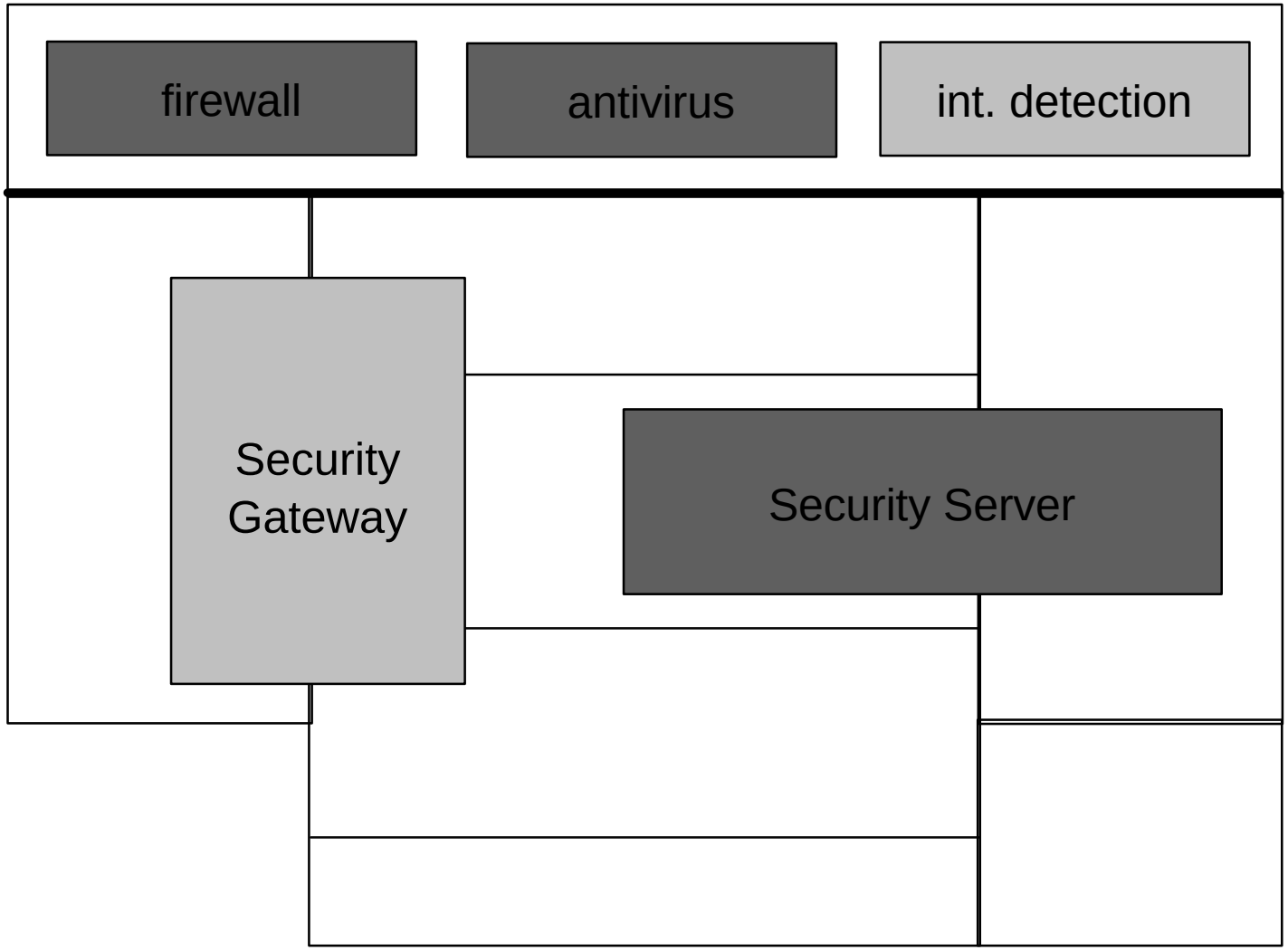
What is DSSeries Security?

Requirement	Function	Technology
Authorization	Data Protection	Key Distribution
		Origin Authentication
		Data Privacy
		Data Integrity
	Access Control	Policy Enforcement
		Privilege Management
		User Authentication
Accountability	Audit	
		Event Generation/Disposition
	Non-Repudiation	Data Signature
		Trusted Time
Availability	Service Continuity	Replication
		Resource Quotas
		Rate Limitation
	Disaster Recovery	Data Backup / Restore
		Key Recovery
Assurance	Engineering Practice	Design / Test / Verify
	Development Process	Documentation
	Operations Management	Integrity Maintenance & Restoration
Administration	System Configuration	Install / Configuration / TCB Mgmt.
	Mechanism Management	Activation / Defaults
	Policy Management	User, Authorization, Audit, Trust, ...

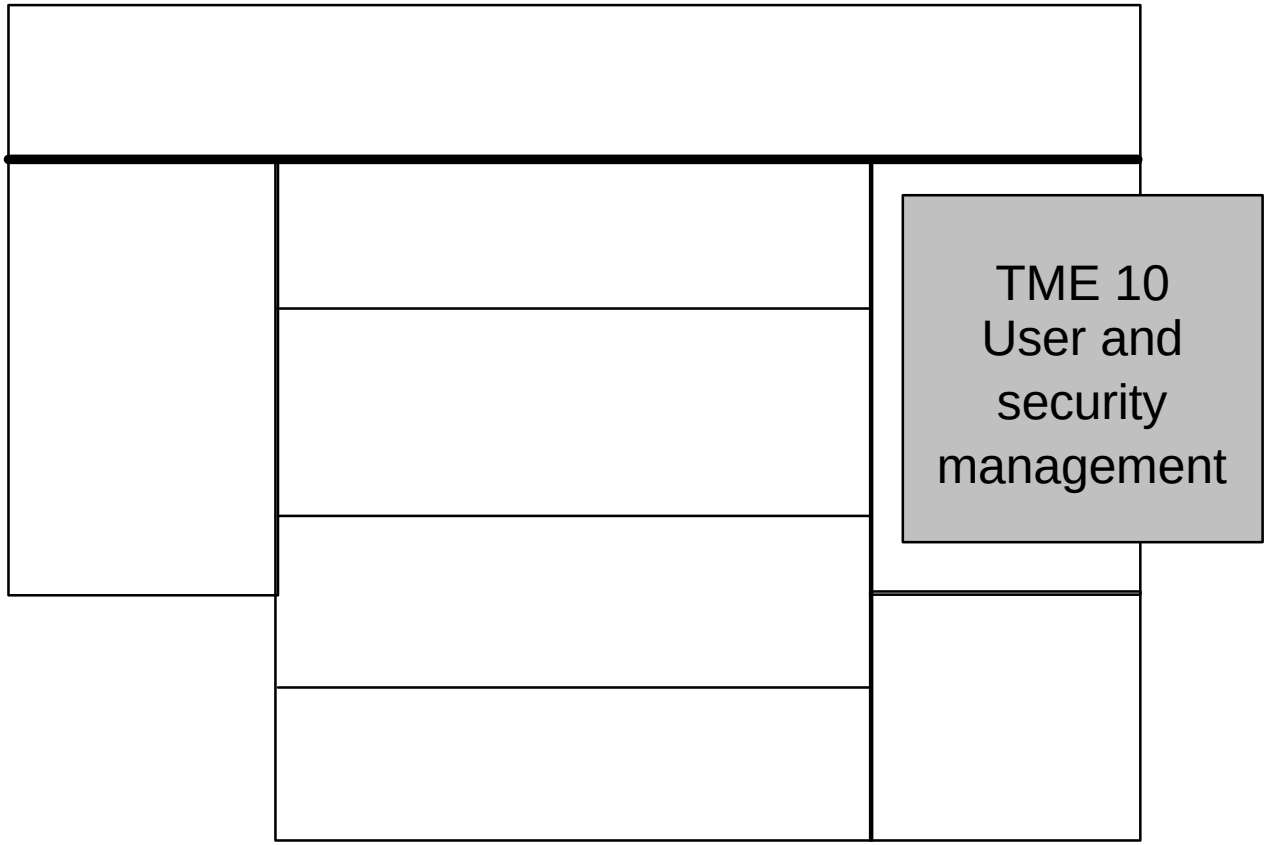
DSSeries Security: GSO



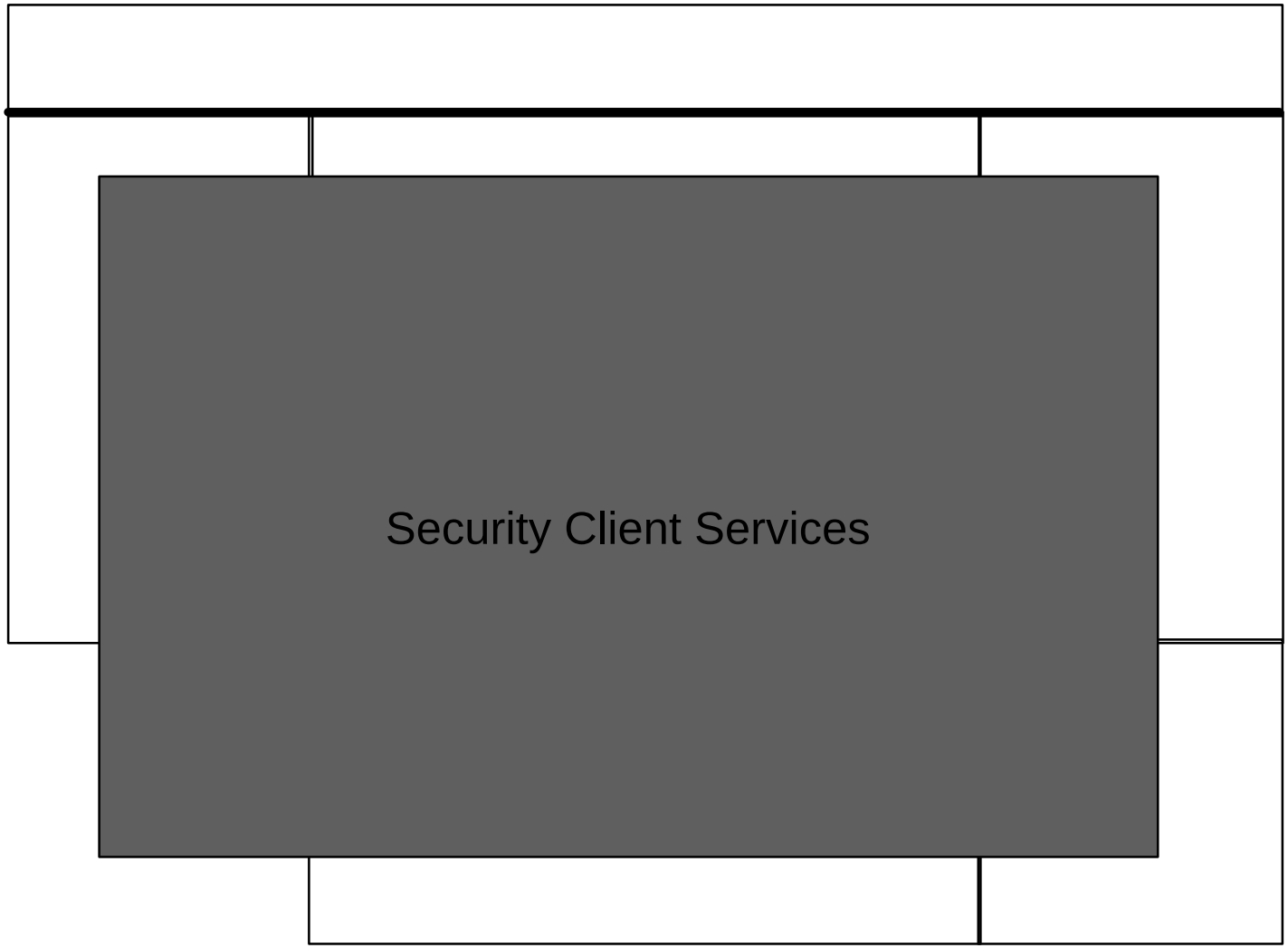
DSSeries Security: Enterprise Services



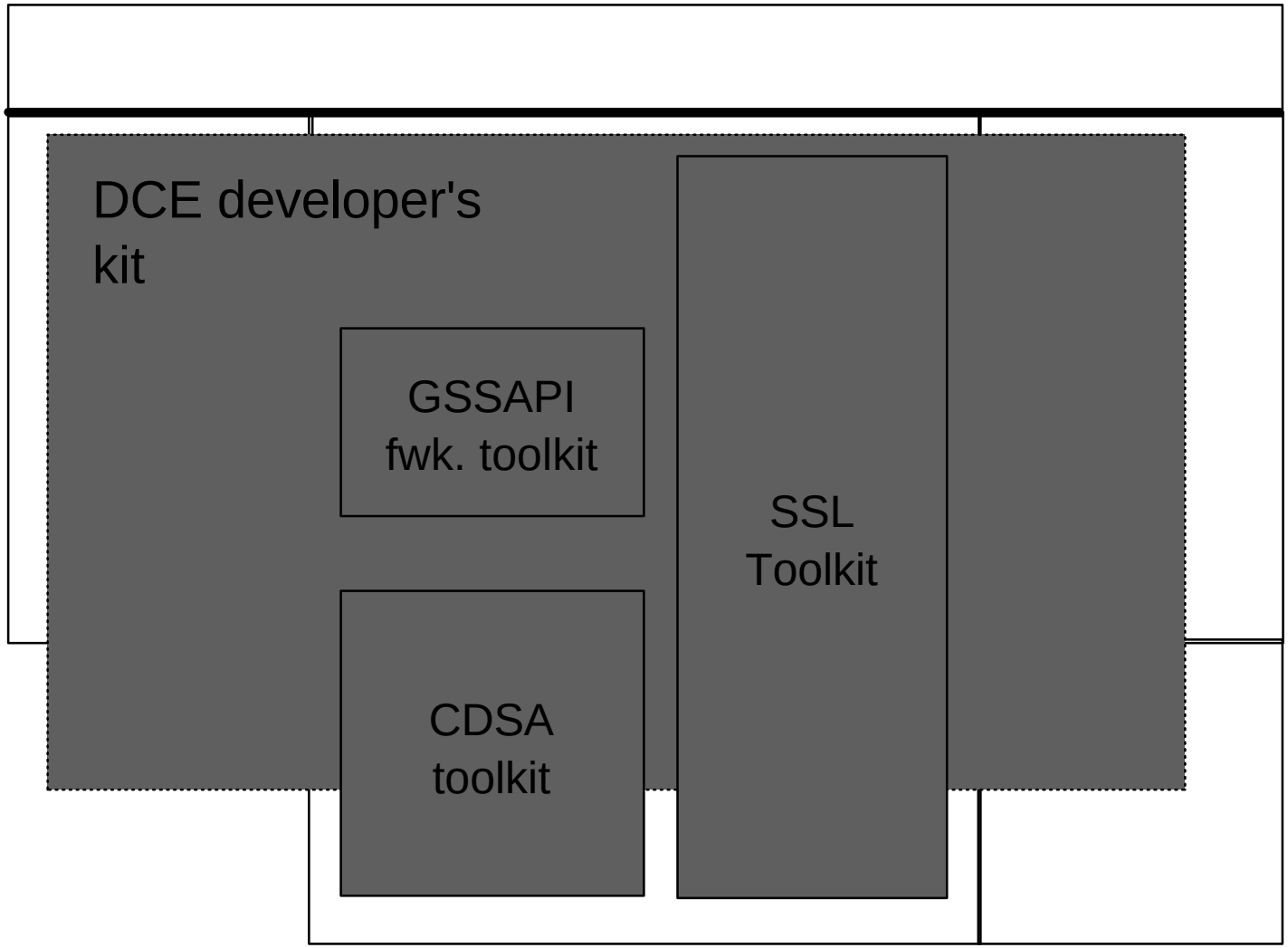
TME 10



DSSeries Security: Client Services



DSSeries Security: Developer Tools



Where can I Learn More (1 of 3)?

Architecture for Public-Key Infrastructure

http://www.rdg.opengroup.org/public/tech/security/pki/apki_1-0.pdf

CORBAsecurity

http://www.omg.org/pub/docs/formal/97-02-20.pdf

http://www.omg.org/pub/docs/formal/97-02-21.pdf

CSSM (CDSA)

http://developer.intel.com/ial/security/security/cdsa/cssm.htm

XSSO

http://www.rdg.opengroup.org/public/tech/security/sso/index.htm

***Compliance Defects in Public-Key Cryptography*, by Don Davis**

http://www.usenix.org/publications/libraray/proceedings/sec96/davis.html

(USENIX membership required for access to full paper; abstract free)

Economic Modelling and Risk Management in Public-Key Infrastructures

http://www.chait-amyot.ca/docs/pki.html

Where can I Learn More (2 of 3)?

PKIX

http://www.ietf.org/html.charters/pkix-charter.html

Java security

http://www.javasoft.com/security/

LDAP

http://www.ietf.org/html.charters/asid-charter.html

GSS-API, IDUP-GSS-API

http://www.ietf.org/html.charters/cat-charter.html

PCSC

http://www.smartcardsys.com/

SSL

http://home.netscape.com/eng/ssl3

Security Multipart

ftp://ftp.internic.net/rfc/rfc1847.txt

X.509v3 Certificate Format

http://www.entrust.com/downloads/x509v3.pdf

Where can I Learn More (3 of 3)?

PKCS Standards

http://www.rsa.com/rsalabs/pubs/PKCS/

Some General PKI Links

http://www.pca.dfn.de/eng/team/ske/pem-dok.html
http://csrc.ncsl.nist.gov/pki/
http://www.xcert.com/~marcnarc/PKI/index.htm
http://www.esat.kuleuven.ac.be/cosic/sesame.html
http://www.oecd.org/dsti/iccp/legal/priv-en.html
http://www.oecd.org/dsti/iccp/crypto_e.html
http://www.rdg.opengroup.org/public/tech/security/pki/index.htm