HP Key Management Overview

IEEE Key Management Summit
September 23-24, 2008

Mark Schiller – HP Security Program Office, HP Secure Advantage
Steve Wierenga – HP Security Products Group, HP Secure Advantage

Speaker Bio

Mark Schiller

- Mark Schiller is the director of the HP Security Office, responsible for coordinating HP's security standards strategy, within HP's Secure Advantage program. Schiller additionally drives HP's Trusted Computing Strategy for HP and represents HP to government and public policy groups, on the topics of Trust and Security. Schiller has worked on security, operating systems, clients, servers, high-availability and telephony.

Steve Wierenga

- Steve is an HP Distinguished Technologist and serves as architect and technical lead for key management for HP's Secure Advantage program. He holds 17 patents in fault tolerant systems and security.

Agenda

- HP's Secure Advantage Program
- HP's enterprise data security vision:
  - ubiquitous data protection, encryption, key management
  - strong security policy controls and auditability
- HP's enterprise KM strategy
- HP StorageWorks Secure Key Manager
- HP/partner client interoperability
- Q+A

HP in today's security market
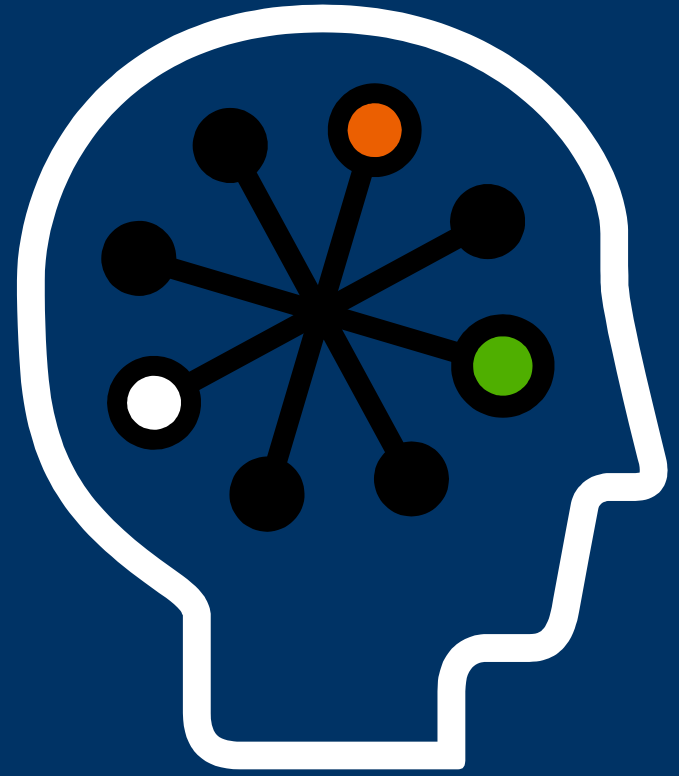
"Companies of all sizes are grappling with how to handle increased business risks associated with data center sprawl, network attacks and new regulatory pressures."

"The breadth of HP's Secure Advantage portfolio, combined with its services strength, addresses evolving challenges with security and compliance."

John Oltsik

Senior information security analyst, ESG

HP delivering solutions to security needs!

✓ HP has been protecting the majority of the world's financial data for 35 years—the same technology and expertise is now being applied to vertical industries

✓ HP has a global installed base of hardened infrastructure components that process and retain massive amounts of sensitive business, customer and employee data

✓ HP provides a full range of solutions that deliver integrated security, from desktop to data center, now called HP Secure Advantage
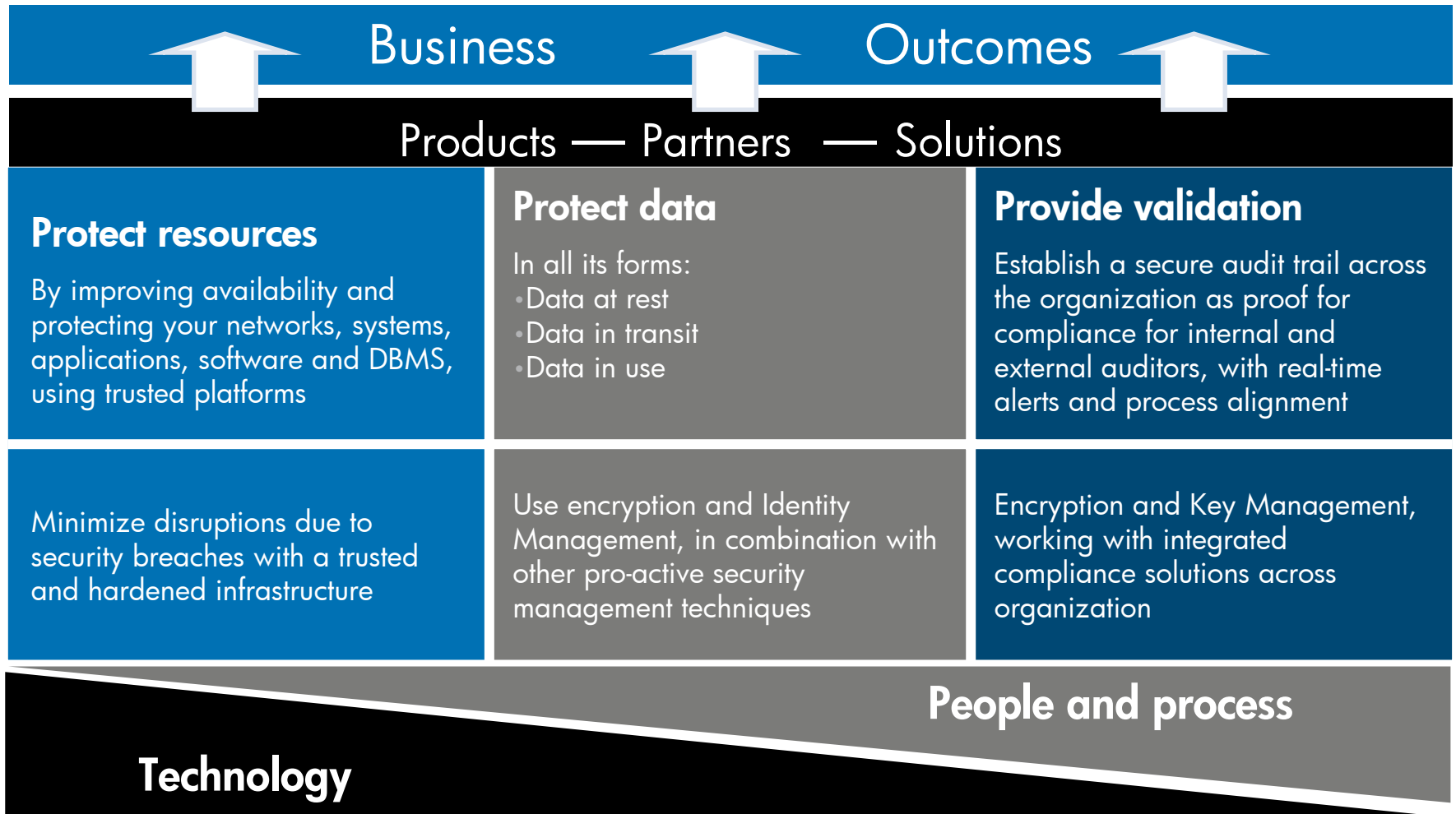
✓ HP enables customers to become compliant with prevailing industry requirements, integrating partners and HP solutions for you.

✓ HP Services uses HP internal Best Practices and HP Labs Technologies to create and commercialize Security solutions and services for customers

HP Secure Advantage Solutions enable business outcomes

The secure end-to-end business advantage

Business Outcomes

Products — Partners — Solutions

Protect resources

By improving availability and protecting your networks, systems, applications, software and DBMS, using trusted platforms

Minimize disruptions due to security breaches with a trusted and hardened infrastructure

Protect data

In all its forms:
- Data at rest
- Data in transit
- Data in use

Use encryption and Identity Management, in combination with other pro-active security management techniques

Provide validation

Establish a secure audit trail across the organization as proof for compliance for internal and external auditors, with real-time alerts and process alignment

Encryption and Key Management, working with integrated compliance solutions across organization

People and process

Technology

HP Secure Advantage portfolio

Protect resources

- PE Vulnerability and Patch Management Pack
- HP Host Protection Essentials-IDS, IPS, +
- NonStop Safeguard
- Neoview Secure remote monitoring
- HP Configuration Management Solution
- HP ProCurve Network Access Control
- HP Live Network

- HP OpenVMS
- HP-UX 11i – CC EAL4+ HP-UX EVFS, RBAC, Plus
- Linux CC LSPP, RBACPP, CAPP EAL4+
- HP Application Security Center
- HP ProtectTools
- HP NetTop
- HP Secure Print Advantage
- HP ProCurve Network Immunity Manager

- HP Security Services
- HP TCS for Energy
- HP Compliance Log Warehouse

Protect data

- HP StorageWorks Secure Key Manager
- LTO-4 Tape products with embedded encryption
- HP Systems Insight Manager
- HP Data Protector Express v3.5 / Data Protector v6.0 w/encryption
- HP StorageWorks Medical Archive Solution
- HP ISA Server
- HP Storage Tape Interoperability with Decru and Neoscale
- HP NonStop Volume Level Encryption-DataFort
- HP Drive Encryption for Protect Tools
- HP Firewall/VPN Server – Check Point Edition
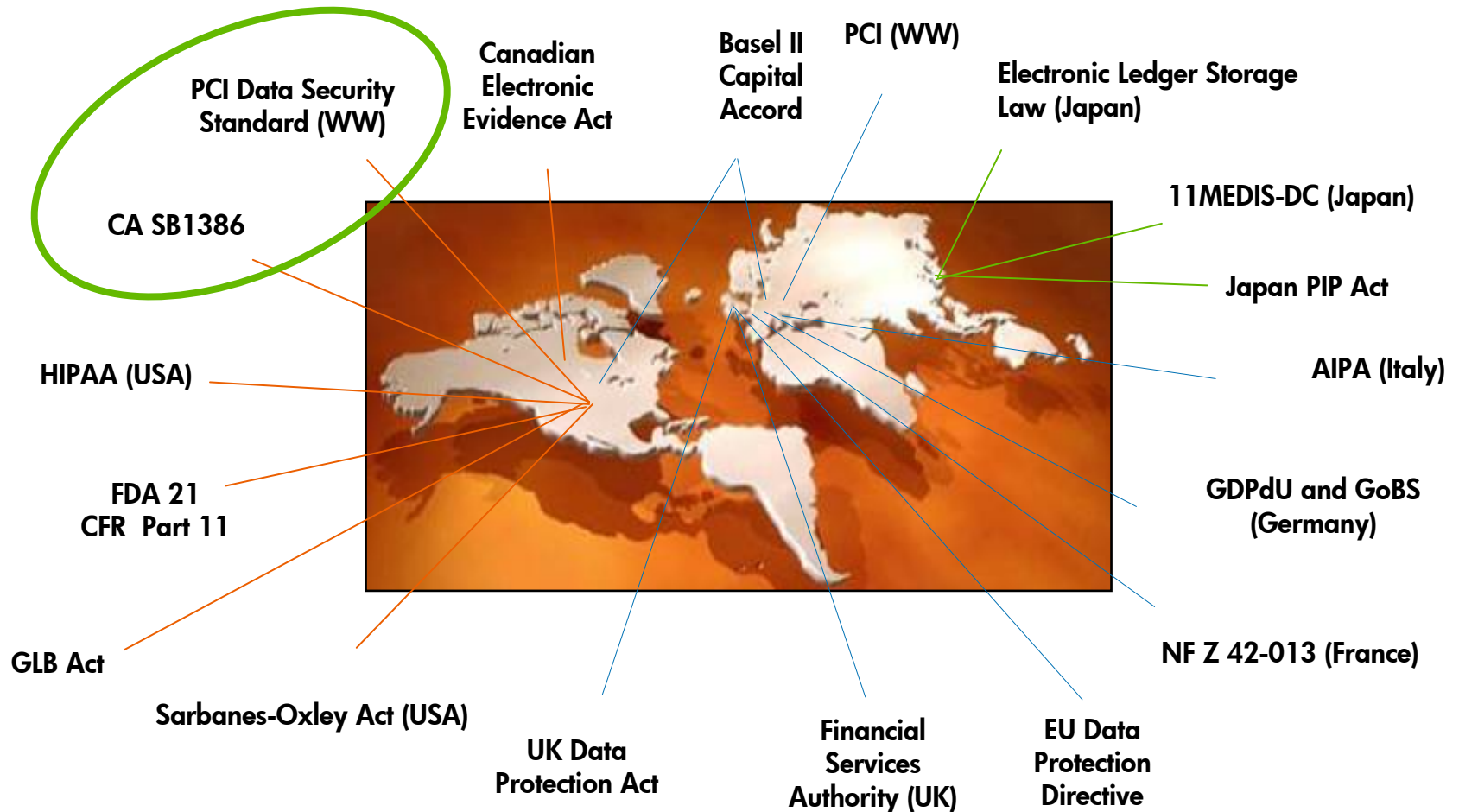- HP ProCurve Identity Driven Manager

- HP ILM for E-mail
- HP Atalla Key Block, NSP

- RIM/RIM4DB
- HP ProCurve Manager
- HP Information Security Service Management
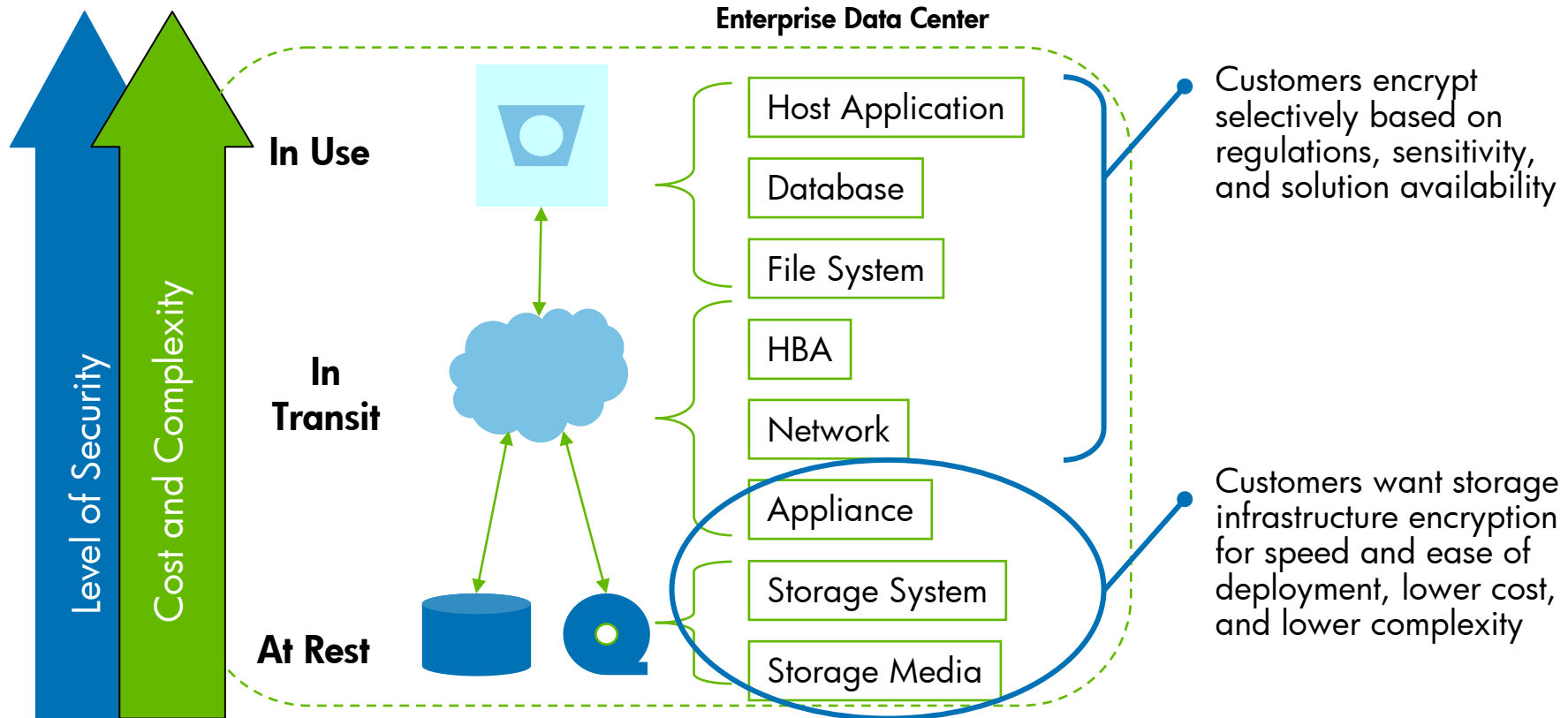
Provide validation

Why Encrypt?
Enterprise data security mandates

PCI Data Security Standard (WW)

CA SB1386

Canadian Electronic Evidence Act

Basel II Capital Accord

PCI (WW)

Electronic Ledger Storage Law (Japan)

11MEDIS-DC (Japan)

Japan PIP Act

AIPA (Italy)

HIPAA (USA)

FDA 21 CFR Part 11

GLB Act

Sarbanes-Oxley Act (USA)

UK Data Protection Act

Financial Services Authority (UK)

EU Data Protection Directive

GDPdU and GoBS (Germany)

NF Z 42-013 (France)

Note: International companies must adhere to regulations in each country of operation

Protecting sensitive enterprise data

Multiple encryption options motivate a unified key management framework

Enterprise Data Center

Level of Security

Cost and Complexity

In Use

In Transit

At Rest

Host Application

Database

File System

HBA

Network

Appliance

Storage System

Storage Media

Customers encrypt selectively based on regulations, sensitivity, and solution availability

Customers want storage infrastructure encryption for speed and ease of deployment, lower cost, and lower complexity
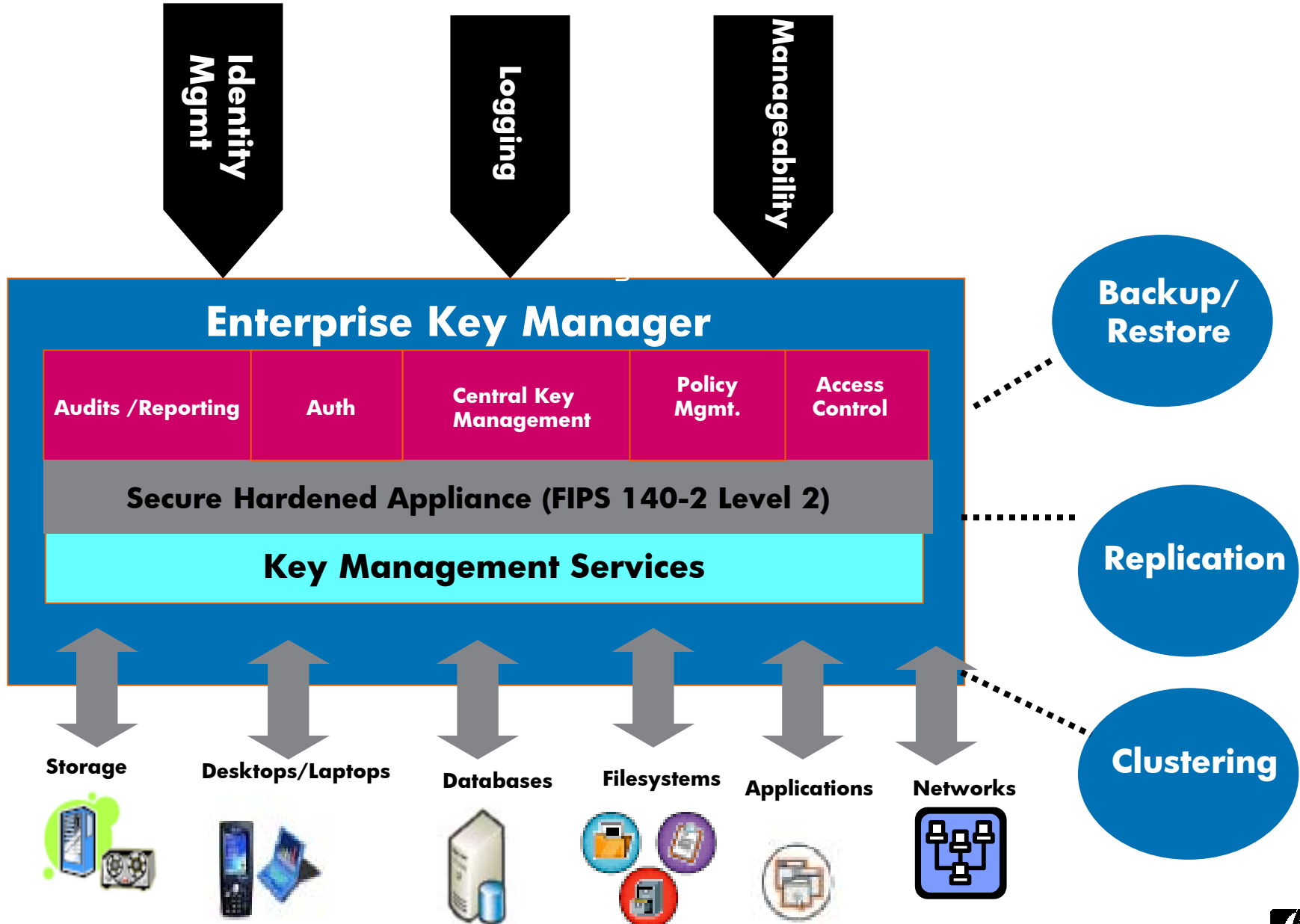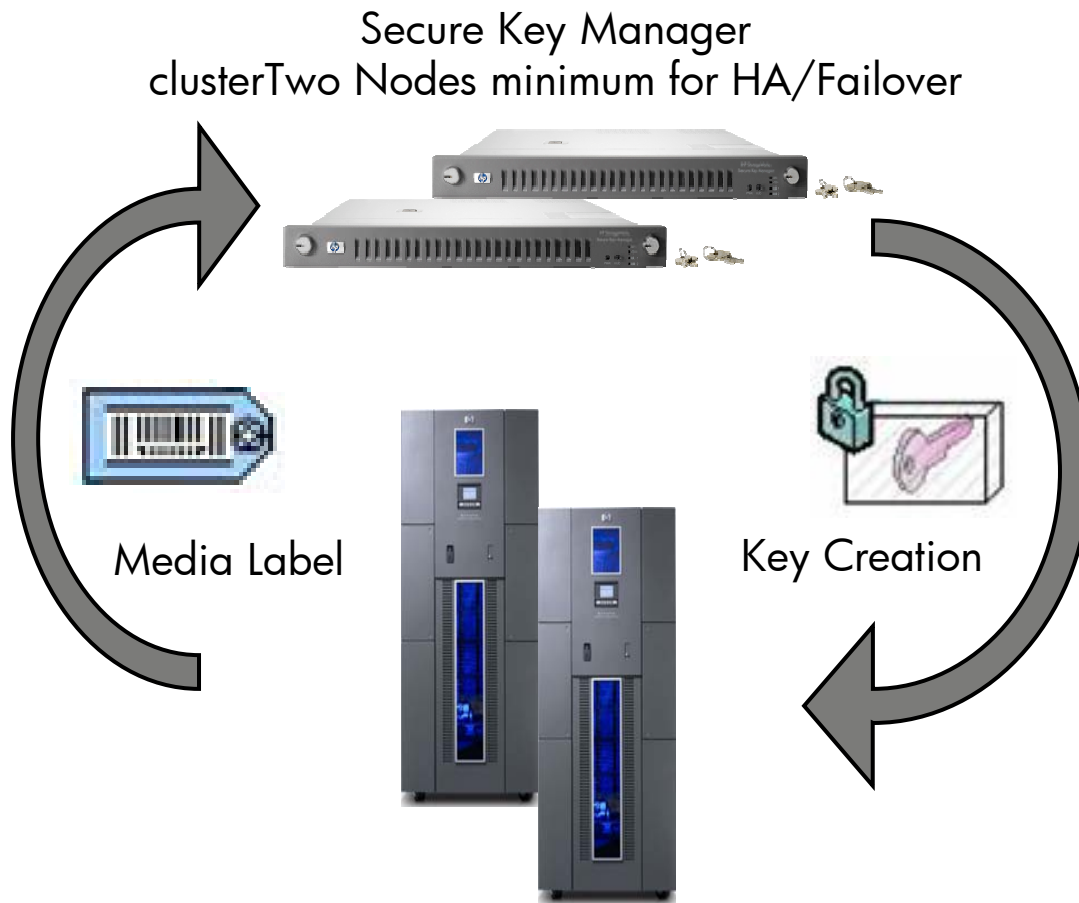
Enterprise Key Management

What is it, who needs it, why is it important ?

- If you're not protecting the keys, encryption is not protecting your data !
- If you're not preserving the keys, encryption is erasing your data !
- If you can't securely move keys across the enterprise, your encrypted data is not accessible !
- If you can't centrally control, automate, and audit your data protection policies, encryption is a wasted investment !

HP Key Management Framework/Vision

Identity Mgmt

Logging

Manageability

Enterprise Key Manager

Audits /Reporting	Auth	Central Key Management	Policy Mgmt.	Access Control

Secure Hardened Appliance (FIPS 140-2 Level 2)

Key Management Services

Backup/ Restore

Replication

Clustering

Storage

Desktops/Laptops

Databases

Filesystems

Applications

Networks

HP Key Management Programs

Encryption keys are easy to deploy and manage

Secure Key Manager
clusterTwo Nodes minimum for HA/Failover

Media Label

Key Creation

- Security officer configures **Secure Key Manager**, enrolls tape library and creates key management policy
- Tape library retrieves keys automatically from Secure Key Manager with unique id.
- Keys are automatically replicated between nodes and across sites.
- All key management operations are recorded in a digitally signed log for audit.

What customers want in KM solutions

High security, availability, reliability

High usability, automation

Enterprise capacity and scale

Investment protection

- Trusted, stable supplier
- Interoperability with wide range of KM clients
- Independent standards and security validations
- Platform for the future

HP KM leadership

KM server products and plans

KM client product roadmaps

SA KM client development program

KM standards support

Only HP: Desktop to Datacenter, Mobile to Print

HP StorageWorks® Secure Key Manager

Security Appliance

- hardened Linux platform
- software pre-installed
- FIPS 140-2 Level 2 validated
- dual security officer controls
- signed event/audit logs

High Availability

- redundant power, mirror disks
- failover cluster, 2-20+ nodes
- keys, policies auto propagated

Client KM Services

- certificate-authenticated TLS session
- generate, export, import keys
- share keys among client groups
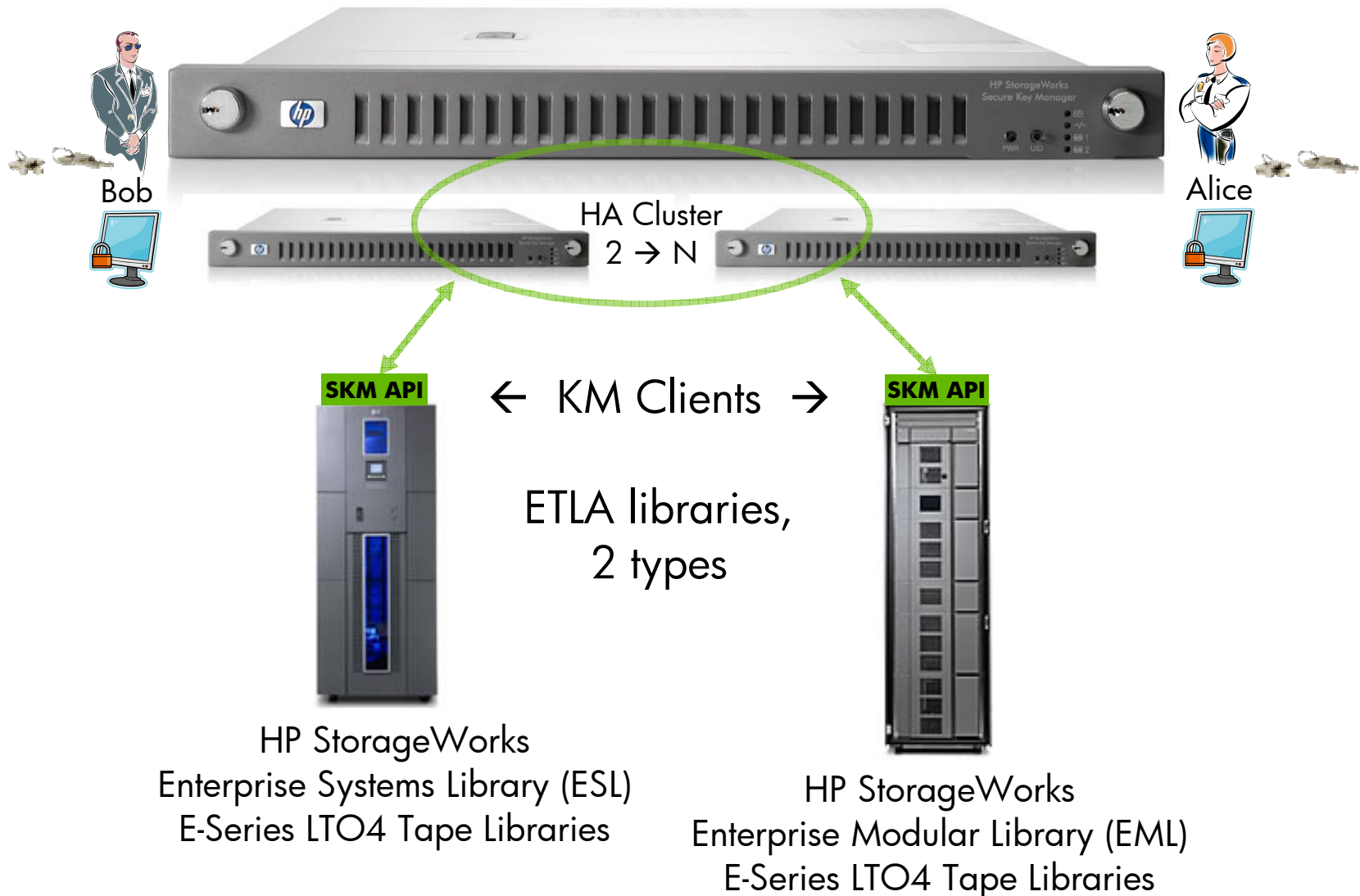- serve 100K – 1M+ keys, metadata

Administrative Services

- configure, set policies, establish CA
- enroll users/clients, issue certificates
- manage groups, privileges, policies
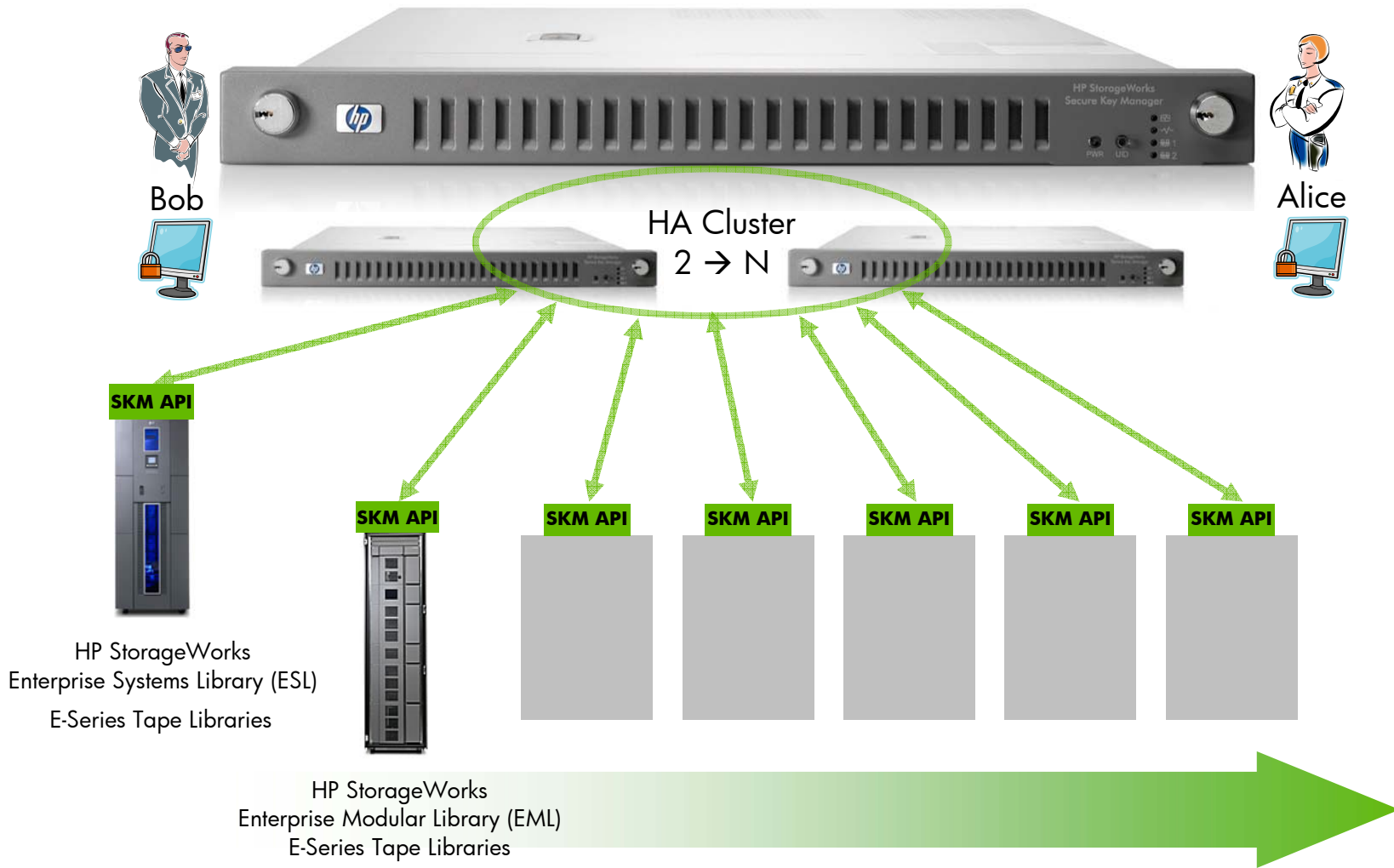- rotate logs, secure backup/restore

http://h18006.www1.hp.com/products/storageworks/secure_key/index.html

HP Secure Key Manager

Bob

Alice

HA Cluster
2 → N

SKM API ← KM Clients → **SKM API**

ETLA libraries,
2 types

HP StorageWorks
Enterprise Systems Library (ESL)
E-Series LTO4 Tape Libraries

HP StorageWorks
Enterprise Modular Library (EML)
E-Series LTO4 Tape Libraries

HP Secure Key Manager 2007-2009

Bob

Alice

HA Cluster
2 → N

SKM API

SKM API

SKM API

SKM API

SKM API

SKM API

SKM API

HP StorageWorks
Enterprise Systems Library (ESL)

E-Series Tape Libraries

HP StorageWorks
Enterprise Modular Library (EML)
E-Series Tape Libraries

HP Key Management Client Strategy

Enable Client–Server interoperability across the enterprise

- Integrate KM Client in all HP enterprise products, HP Secure Advantage Alliance partners:

Datacenter Storage Infrastructure

- Tape Library, SAN Fabric, Disk Array encryption

Datacenter Host Infrastructure

- Application, FileSystem, DataBase encryption
- I/O subsystem, HBA, and device encryption
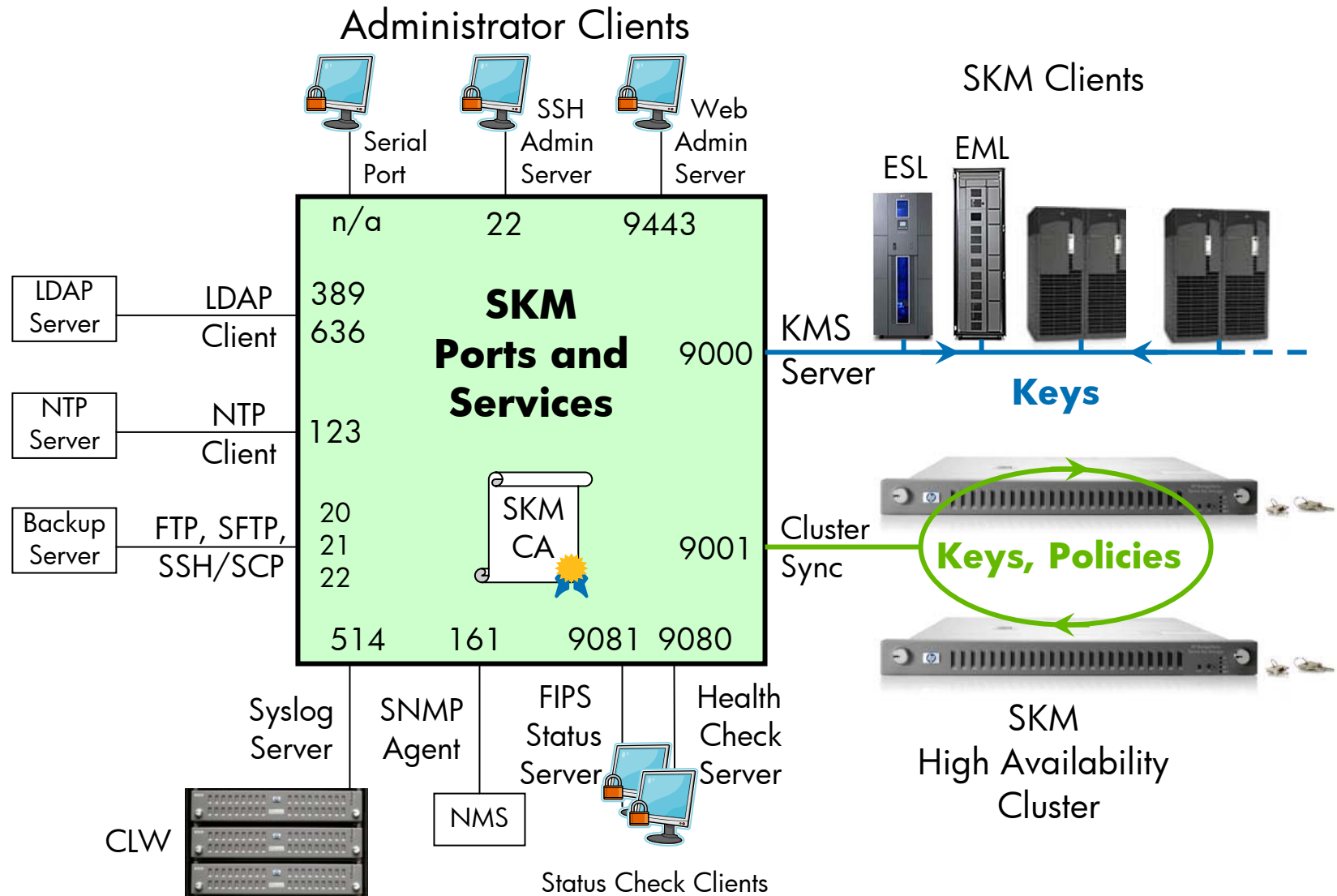- HSMs, blades, encryption offload appliances

Enterprise endpoints

- PCs, Laptops, PDAs
- Printers

Secure Key Manager Ports and Services

Administrator Clients

SKM Clients

	Serial Port	SSH Admin Server	Web Admin Server
	n/a	22	9443

ESL   EML

SKM Ports and Services

LDAP Server — LDAP Client — 389 / 636

NTP Server — NTP Client — 123

Backup Server — FTP, SFTP, SSH/SCP — 20 / 21 / 22

SKM CA

KMS Server — 9000 — **Keys**

Cluster Sync — 9001 — **Keys, Policies**

514	161	9081	9080

Syslog Server   SNMP Agent   FIPS Status Server   Health Check Server

CLW

NMS

Status Check Clients

SKM High Availability Cluster

SKM Client SDK contents

SKM Client library source and object code
- SKM client C source and object library package (Linux, Unix, Windows)
- SKM client Java source and object library package (Linux, Unix, Windows)

SKM and Client Documentation
- SKM Users Guide
- SKM Installation Guide, Information poster, Pre-Install Survey
- SKM C API Developer Guide
- SKM Java API Developer Guide
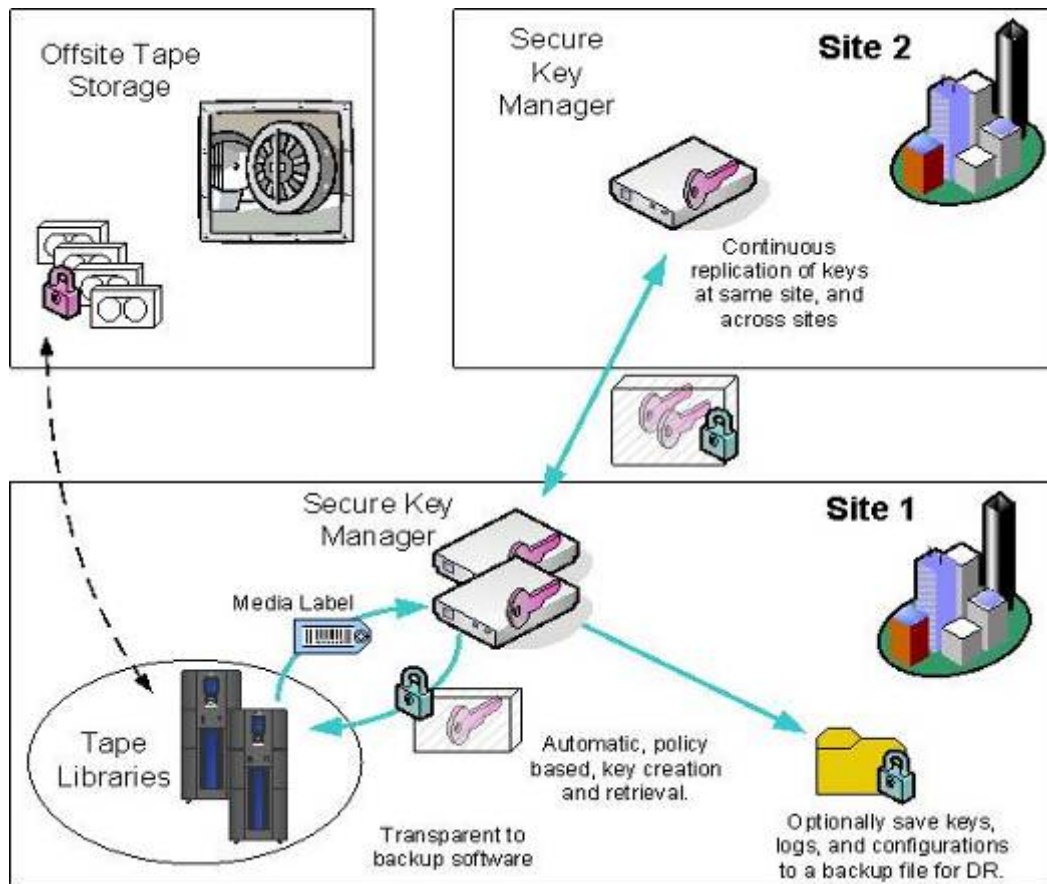- SKM XML Interface Developer Guide

HP Test Tools and Sample Code
- SKM XML Interface Demo tool
- SKM C and Java API Sample Code calling sequences
- SKM Client configuration file samples
- SKM Client validation tests

Developer support
- Developer access to SKM test servers via network or loan units
- 5x8 telephone/email support

Example deployment

HP Secure Key Manager

- Security officer configures Secure Key Manager, enrolls tape library and creates key management policy.

- Tape library retrieves keys automatically from Secure Key Manager based on a unique tape media id.

- Keys are automatically replicated between nodes and across sites.

- All key management operations are recorded in a digitally signed log for audit.

Security announcements at RSA April 7

Protect resource

- HP-UX 11i V3 Common Criteria certifications at the EAL4 level
- HP NetTop 2.1 secure cross-domain release with updated virtualization layer

Protect data

- HP StorageWorks
- C-Series MDS 9000 Storage Media Encryption (SME) fabric switch
- LTO-4 encryption kit for 1/8 G2 Tape Autoloader and MSL Tape Libraries with LTO-4 tape technology
- HP StorageWorks Key Manager integration with HP Compliance Log Warehouse
- Web-based Storage Security Assessment tool

Provide validation

- Mission Critical Security Services (MCSS) offerings from HP Services evaluates information security strategy
- Information Security Service Management (ISSM) reference model expansion for effectively deploying technology infrastructure security
- New PCI vulnerability scanning software product from HP Software's Application Security Center (HP Software Professional Services is certified by the PCI Security Standards Council as an Approved Scanning Vendor)

HP Atalla Cryptographic processing solutions

Protecting resources and data, and providing proof

Atalla Network Security Processors

Optimized for the Atalla Key Block

- Atalla is the market, technology and security leader in security solutions for electronic payment transactions

- HP Atalla NSP products provide unparalleled performance, price and protection

Secure Configuration Assistant

Atalla Trusted Print Center