SHARE Technical Conference

Session 1721

OS/390 Security Trends & Directions

Tying It All Together

Rich Guski, CISSP

(Certified Information Systems Security Professional)

August 22, 1999

IBM OS/390 Security Design and Architecture

Internet: ’guski@us.ibm.com’

(914)435-7753

Enterprise Security Needs

- Internet Trust Model
- Consolidated Security for OS/390 Applications
- Enterprise Security Management
- Enterprise Directory
- Peace of mind

Chart 2

The Need For S/390 Crypto

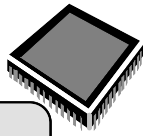
- All this SSL, Certificate, signature, and handshaking is crypto intensive
  - it can eat your processor alive with software crypto processing

- The Solution is **Hardware Crypto**

- **S/390 has it Integrated!**

Chart 3

S/390 CMOS Crypto Coprocessor



- ***Standard feature*** **on Generation 4 and later Parallel Enterprise Servers and Application StarterPak**
- **Integrated support in OS/390 V2**

The Only Server Platform with HW crypto as standard feature

- Offloads crypto operations onto separate high performance engine
- Reduces MIPS usage for crypto intensive operations (e.g., SSL)
- Highly secure storage of critical keys
- Validated by US Gov't NIST at FIPS 140-1 Level 4
  - ***No other vendor in the world has achieved this***
  - **Customers have same assurance as US Gov't can require**

Chart 4

Who uses Crypto on S/390?

S/390 cryptography in use today by:

- WebSphere Application Server for OS/390 (Domino Go Webserver for OS/390)
- IBM CommercePOINT Payment
  - suite of end-to-end commerce solutions on OS/390
- OS/390 Firewall Technology VPN
- OS/390 Security Server DCE Server
- VTAM (e.g., DB2, CICS)
- Financial Institution Applications
- Crypto Based Transactions banking solution
- BSAFE Toolkit - for applications and subsystems
- OS/390 LDAP Server
- OS/390 TN3270 Server
- System SSL
- Open Cryptographic Services Facility (CDSA APIs)

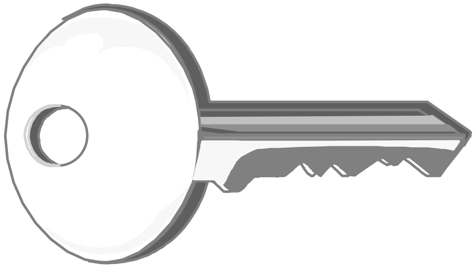
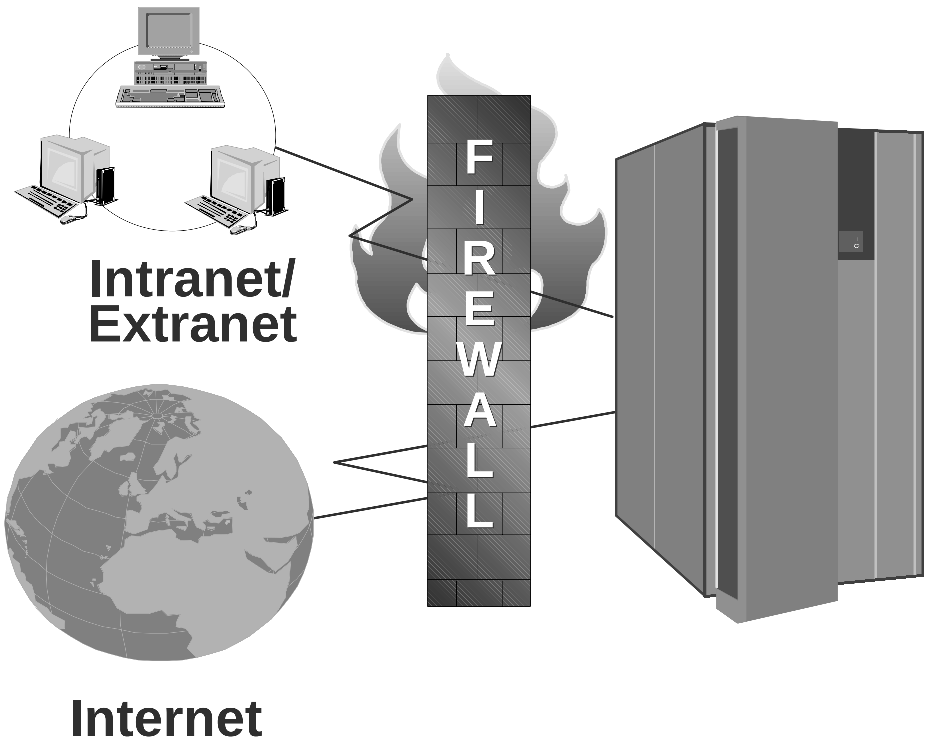


Chart 5

Firewall Technologies

Network Level

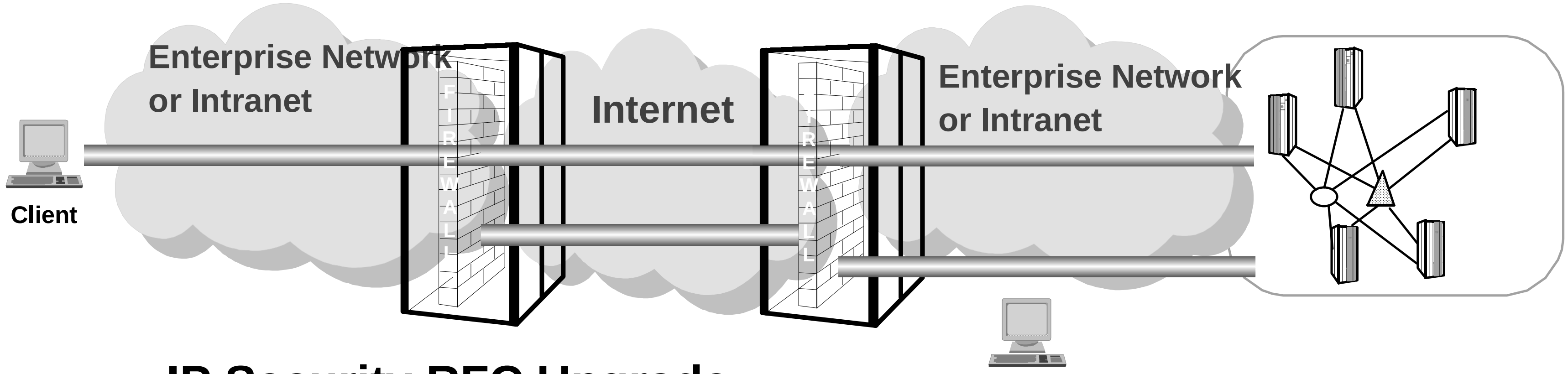


Firewall Technologies

- IP Filtering
- Network Address Translation (NAT)
- Virtual Private Network (VPN) with Crypto HW
- Proxy servers
- SOCKS server
- Domain Name services

Chart 6

IPSec Enhancements (V2R7)



IP Security RFC Upgrade

- Supports latest RFCs (2401-2406, 2410)
  - Maintains interoperability with previous IPSec RFC levels
- Increased security
  - Replay protection added
  - Improved authentication algorithms (HMAC-MD5, HMAC-SHA)

Strong Encryption

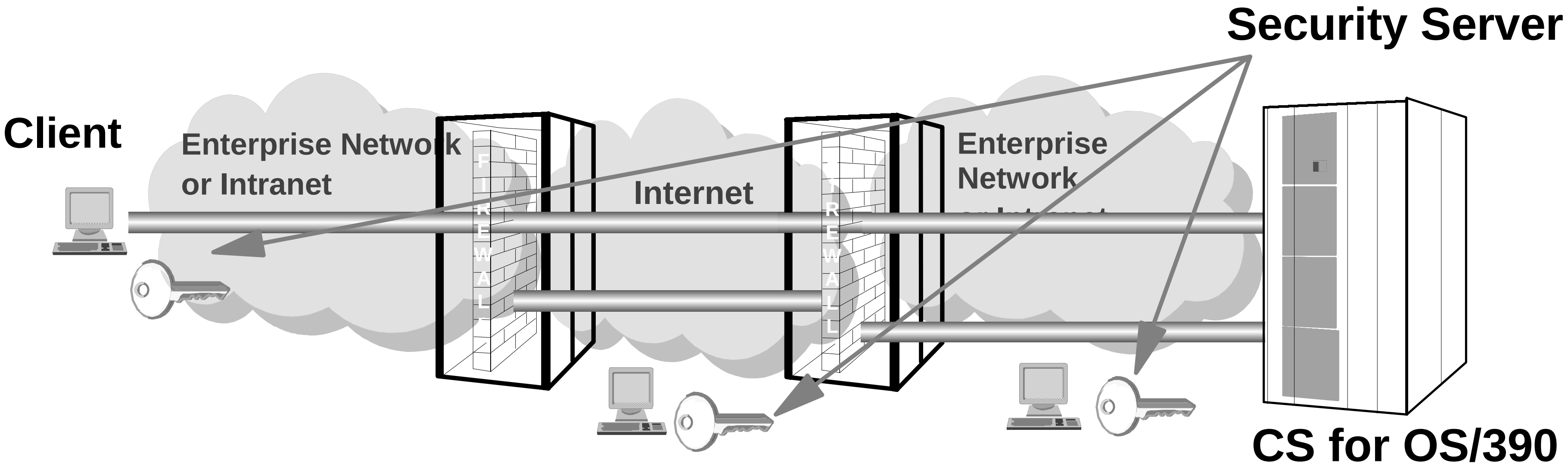
- Triple DES encryption
  - Exploits hardware S/390 cryptographic coprocessor

Configuration improvements

- Client-to-Server security associations
- JAVA-based GUI for IPSec configuration available with Security Server
  - Also configurable through UNIX command line

Chart 7

Key Management (V2R8)



Internet Key Exchange - Simplifies IP Security

- Secure exchange of keys
- Reduces manual configuration
  - Dynamic tunnels
  - A critical element as VPNs grow
- Enables non-disruptive key refresh
- Enables network access with dynamic IP addresses
- Joint offering between the Communications and Security Servers for OS/390

"IKE" formally known as ISAKMP/Oakley

Chart 8

OS/390 Firewall Enhancements

- Release 8
  - Commands to define and manage ISAKMP (Internet Security Association Key Management) protocol
    - Key policies/transforms/proposals: Supports automated generation (and refresh) of tunnel definitions between 2 communicating systems
    - Data policies/transforms/proposals: Authentication of communicating systems is done using either pre-shared key or RSA Signatures (certificates)

- Direction
  - GUI Wizards to aid in ISAKMP configuration
  - Certificate Revocation List (CRL) processing to enhance the security of ISAKMP negotiations

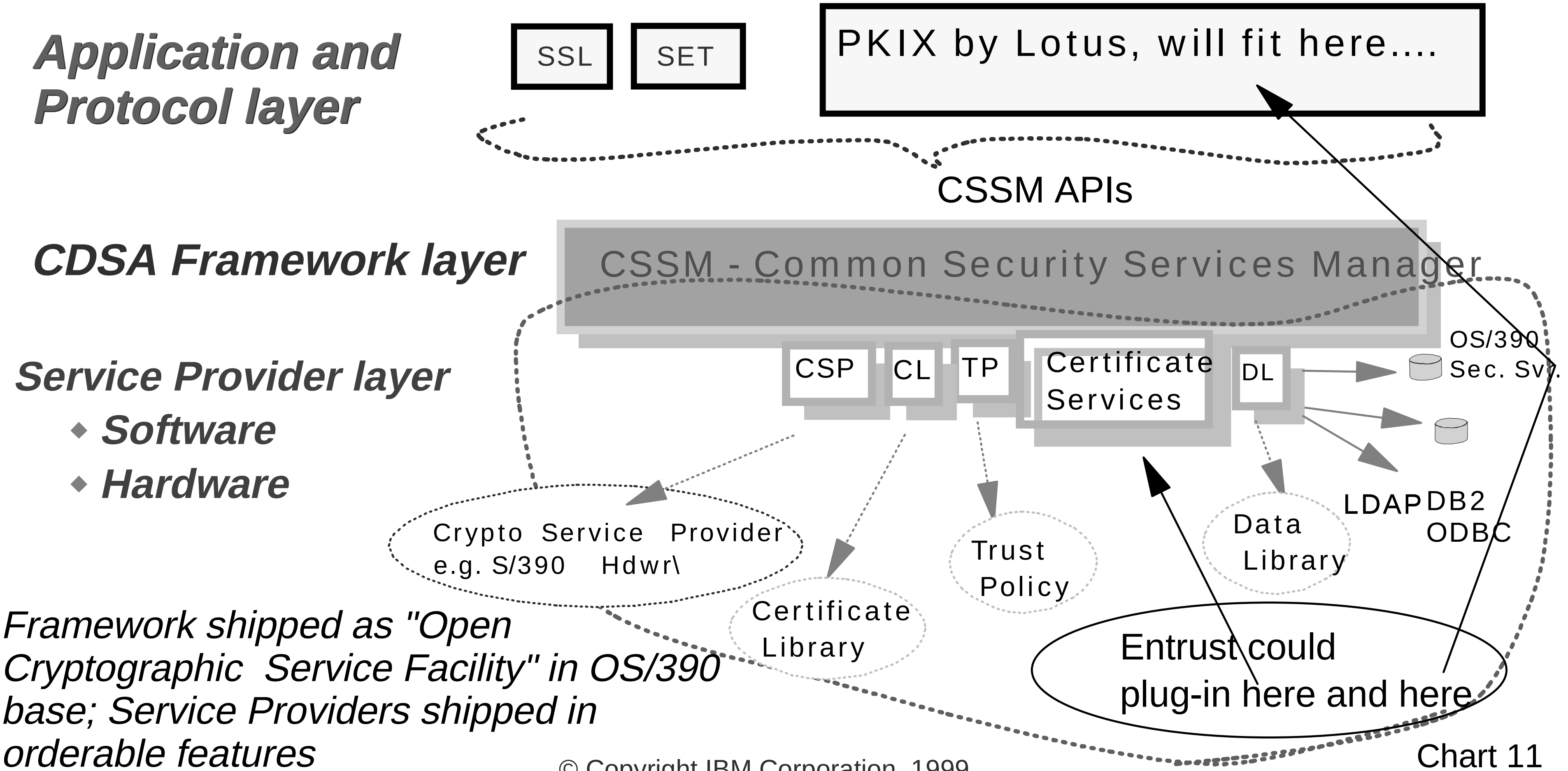
OS/390 Ethical Hacking

- Started in OS/390 R4 with Firewall GA
- Partnership with GSAL (Hawthorn Research)
- Incorporated into OS/390 process as of OS/390 R6
- Focused on CERT security warnings

Chart 10

OCSF (CDSA) Overview

Open Cryptographic Services Facility (OCSF) is an implementation of CDSA. "Common Data Security Architecture": A standard, driven by Intel / IBM / etc. for implementing Crypto data privacy (etc.). CDSA is implemented via CSSM framework and underlying ’service providers’ which, when possible, utilize local hardware.



Application and Protocol layer

SSL

SET

PKIX by Lotus, will fit here....

CSSM APIs

CDSA Framework layer

CSSM - Common Security Services Manager

Service Provider layer

- ***Software***
- ***Hardware***

CSP

CL

TP

Certificate Services

DL

OS/390 Sec. Sv.

LDAP

DB2 ODBC

Crypto Service Provider e.g. S/390 Hdwr\

Certificate Library

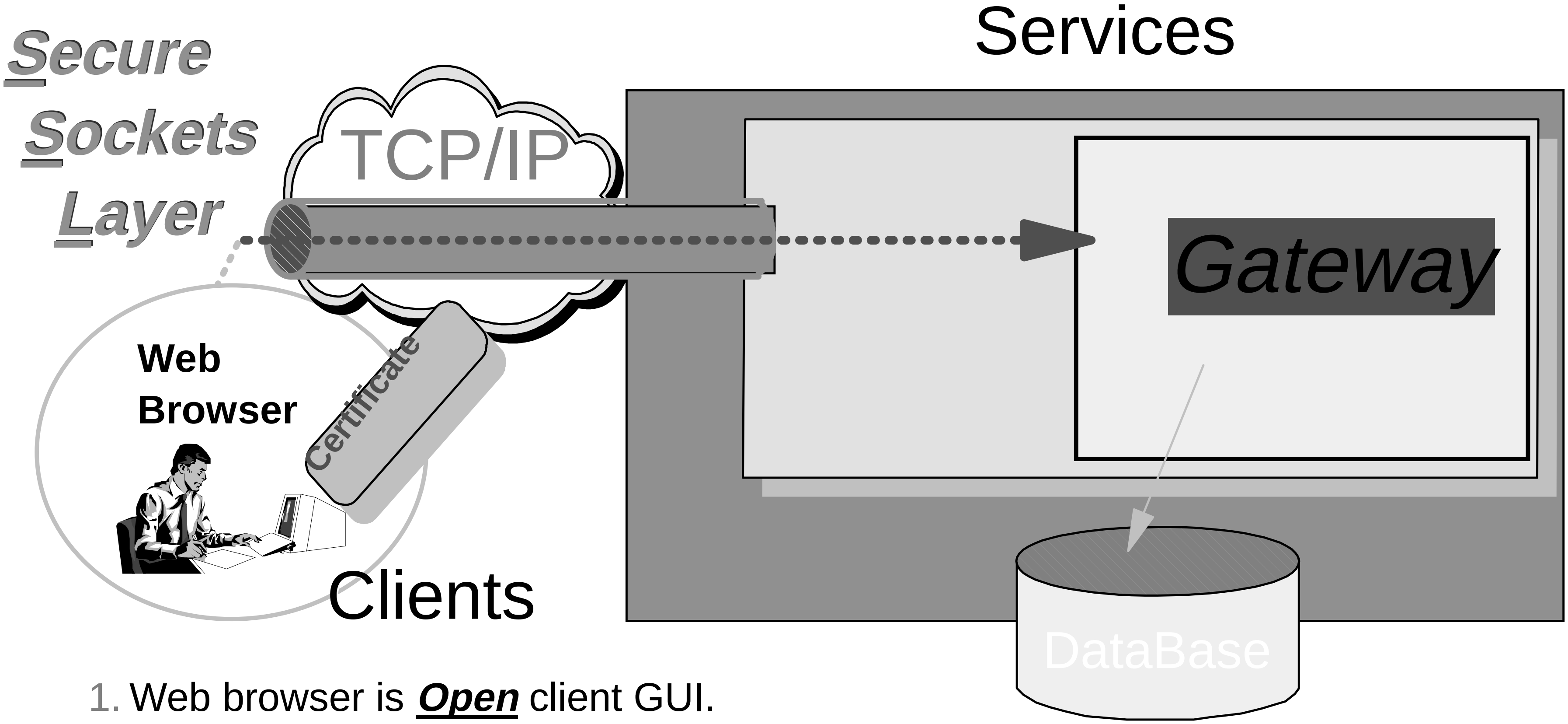
Trust Policy

Data Library

Entrust could plug-in here and here

Framework shipped as "Open Cryptographic Service Facility" in OS/390 base; Service Providers shipped in orderable features

Internet e-Business Model



1. Web browser is ***Open*** client GUI.
2. Consistent browser interface minimize education and costs.
3. Access to any available server that supports HTTP.
4. Easier and less costly to roll out enterprise-wide applications.
5. TCP/IP is commonly supported on most server platforms.

SSL Provides Security

Chart 12

OS/390 Secure Sockets Layer (SSL) Services

- OS/390 introduces a set of services for writing socket applications (client or server-side) that require secure communications - System SSL.

- System SSL is a set of dynamic link libraries (DLLs) that are loaded into calling application’s address space.
  - ►Can be either client or server application on OS/390

- All functions apply to both client and server applications which are using the SSL subsystem services.

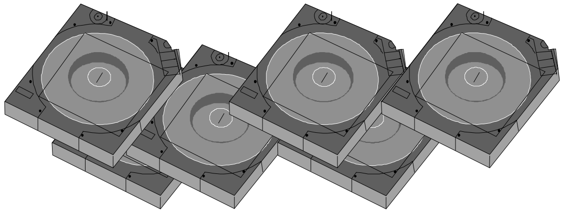
Chart 13

System SSL Release 8

- **RACF support for certificates/keys**
  - Allows customer to consolidate certificates and keys in one place
- **Provide additional security levels**
  - Provide an additional level of exportable encryption capability (56-bit)
  - Keep pace with changes in export regulations
- **SRB support (Direction beyond R8)**
  - Provides versions of gsk_secure_soc_read and gsk_secure_soc_write which can be called in SRB mode.
  - Makes it easier to write programs using SSL and asynchronous I/O.

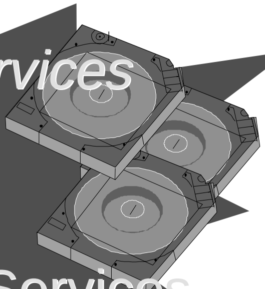
Chart 14

Where CDSA and System SSL fit within OS/390



Base Server Elements

BCP
JES2
OpenEdition (UNIX Services)
ESCON
LANRES/MVS
TSO/E
OSA Support
.....



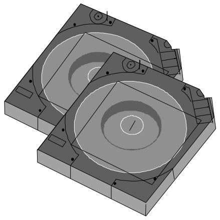
Cryptographic Services

- ICSF
- CDSA*
- System SSL Services

Communication Server Elements

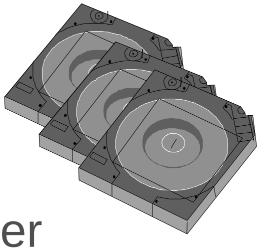
VTAM, TCP/IP,...

Optional Features



C/C++
JES3
RMF

....



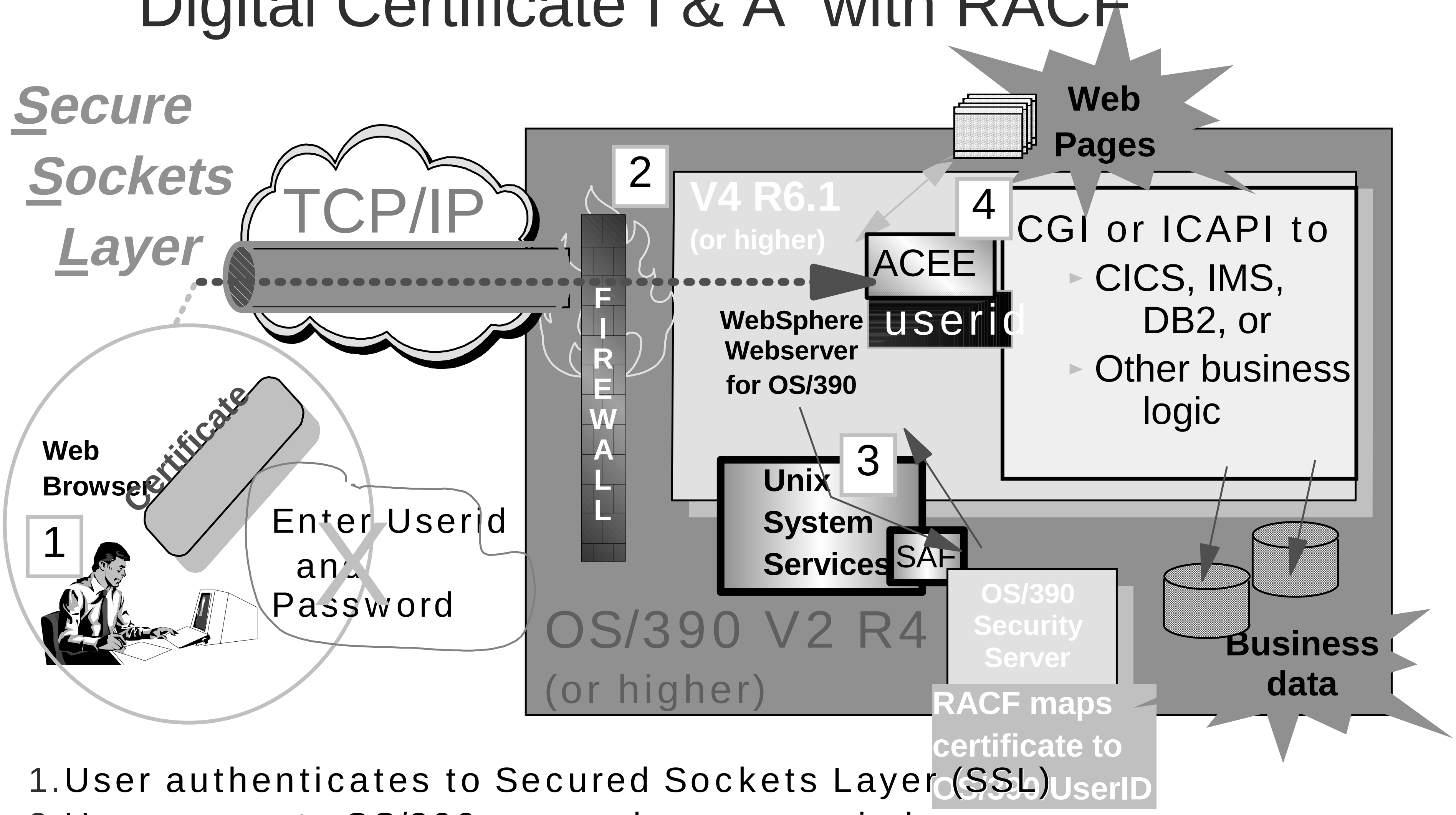
Security Server

- RACF
- DCE Security server
- LDAP Directory Server
- Firewall Technologies

NDS provided with the Security Server

* *Open Cryptographic Services Facility*

Digital Certificate I & A with RACF



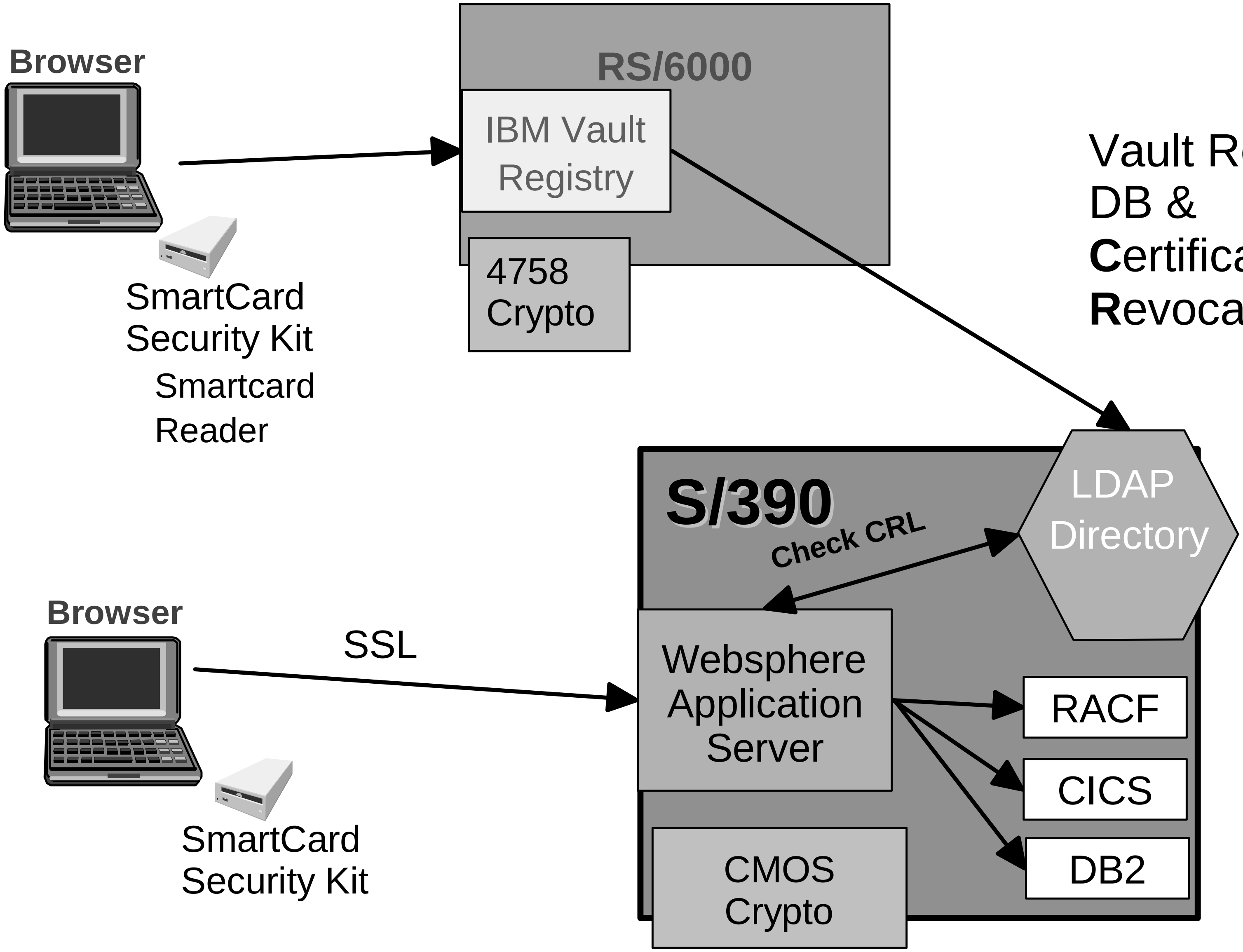
1. User authenticates to Secured Sockets Layer (SSL)
2. User requests OS/390 secured resource via browser
3. OS/390 Web Server invokes RACF via Unix services to build local security context (ACEE), passing SSL validated certificate without the need to prompt for userid & password
4. Business logic executes with identity of the end user

Chart 16

Alcatel Story

- Alcatel extended their Order Status Inquiry system that allows customers to access the status of their order over the Internet.
- 90 percent improvement in response time.
- Around the clock availability.
- Extended a CICS OS/390 application.
- Utilized OS/390 Digital Certificate support & Domino Go WEB Server.
- From concept to rollout in 12 weeks.
- www.software.ibm.com/solutions/internet/G325-1220-00.pdf

OS/390, Vault Registry, Smart Cards



S/390 Security Trust Infrastructure Direction

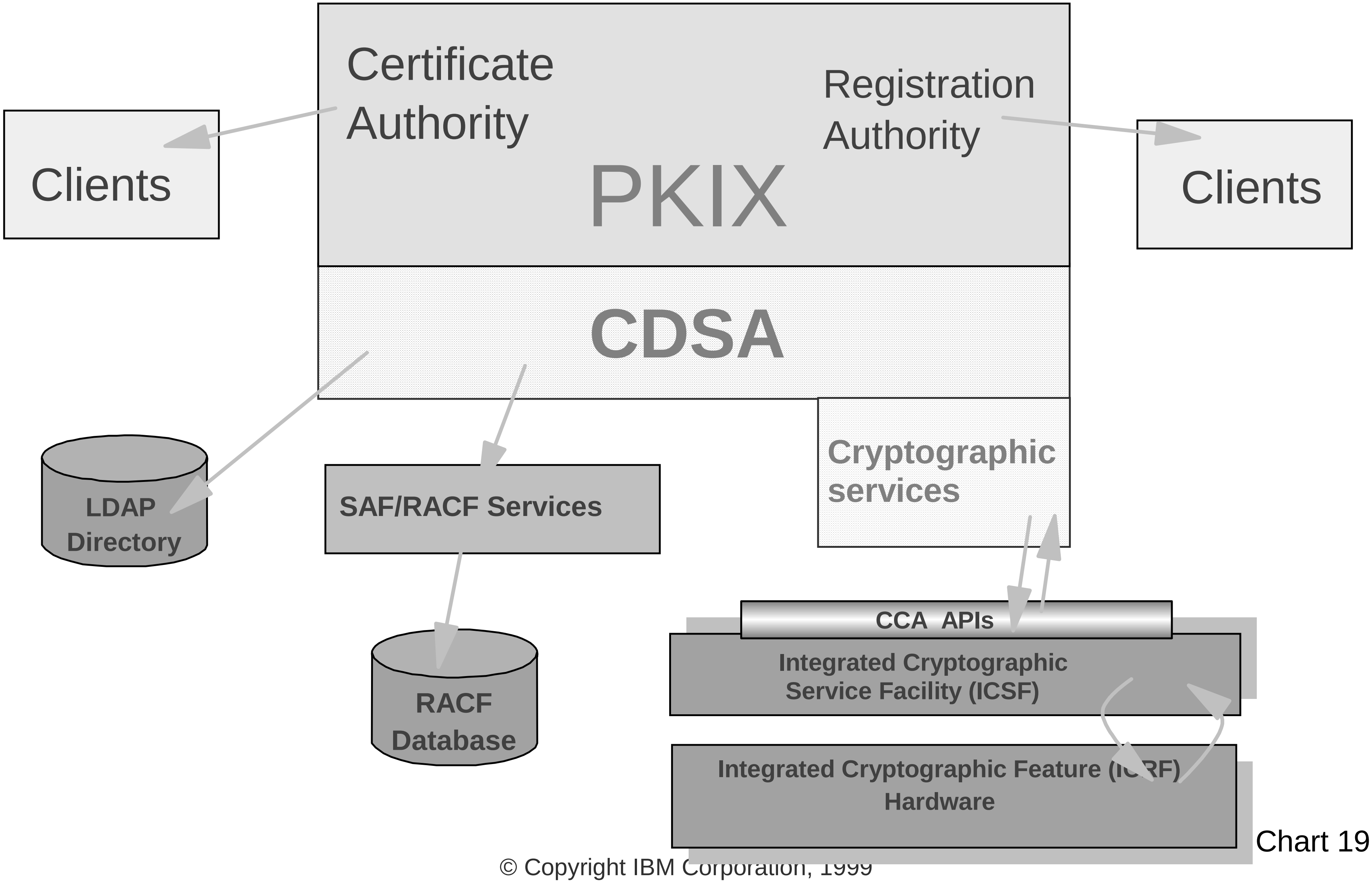
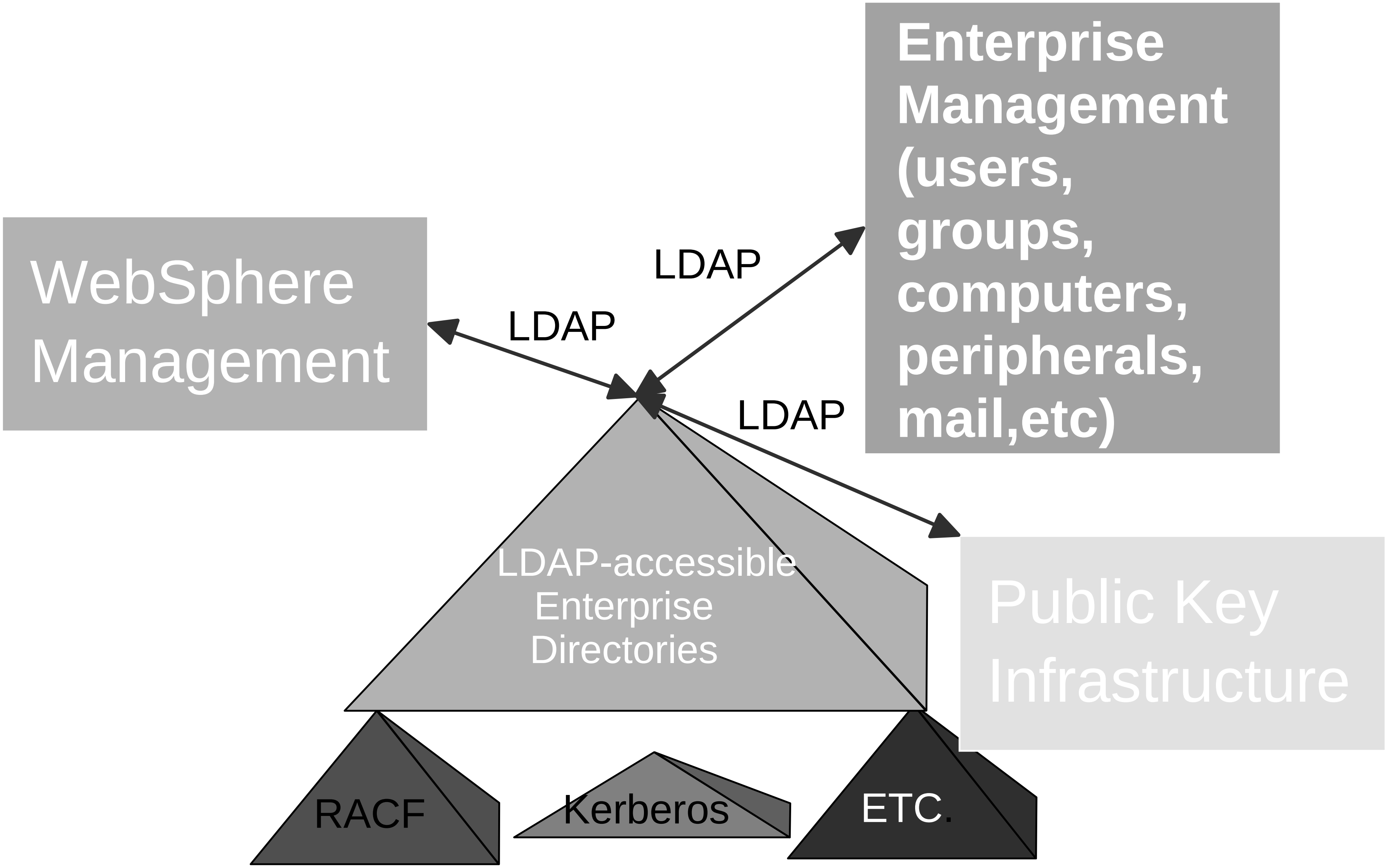


Chart 19

Directories and LDAP



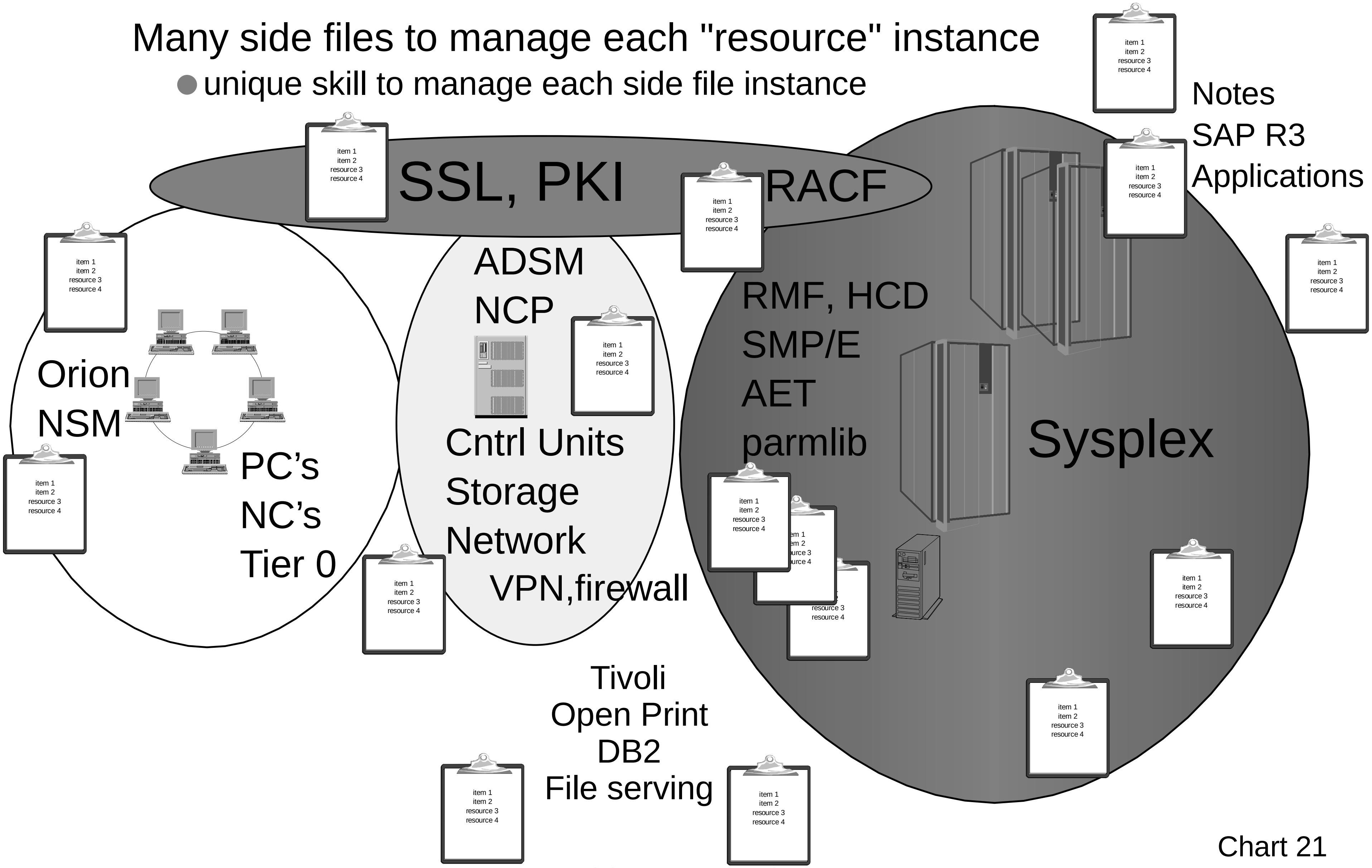
Enterprise Management (users, groups, computers, peripherals, mail,etc)
WebSphere Management
LDAP
LDAP
LDAP
LDAP-accessible Enterprise Directories
Public Key Infrastructure
RACF
Kerberos
ETC.

Chart 20

Typical non-directory enabled business

Many side files to manage each "resource" instance

- unique skill to manage each side file instance



Notes
SAP R3
Applications

SSL, PKI

RACF

Orion
NSM

PC’s
NC’s
Tier 0

ADSM
NCP

Cntrl Units
Storage
Network
VPN,firewall

RMF, HCD
SMP/E
AET
parmlib

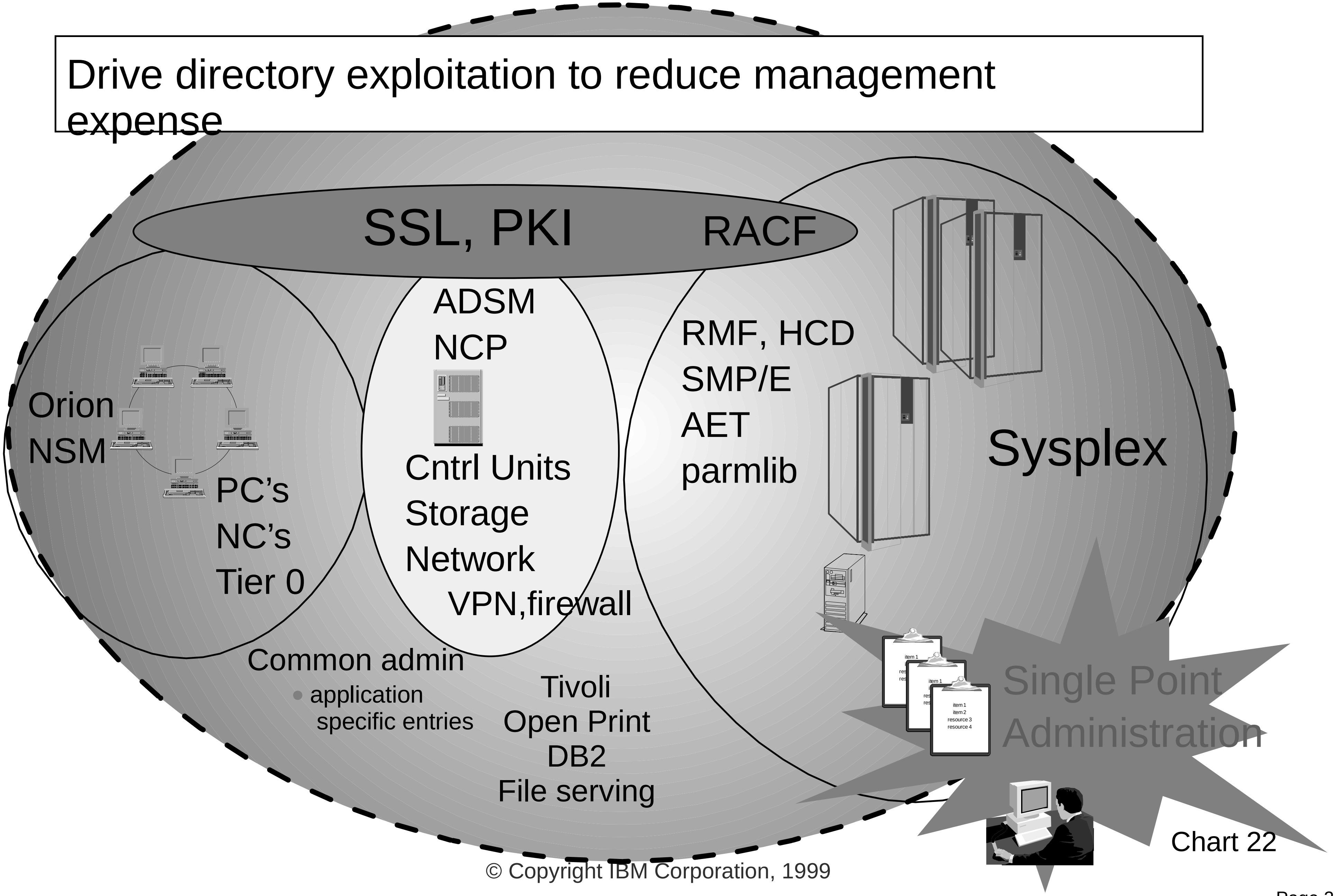
Sysplex

Tivoli
Open Print
DB2
File serving

Chart 21

Directory Enabled Network

Drive directory exploitation to reduce management expense



SSL, PKI RACF

Orion
NSM

PC's
NC's
Tier 0

ADSM
NCP

Cntrl Units
Storage
Network
VPN,firewall

RMF, HCD
SMP/E
AET
parmlib

Sysplex

Common admin
- application specific entries

Tivoli
Open Print
DB2
File serving

Single Point Administration

Chart 22

OS/390 LDAP Support (overview)

- LDAP client
  - ►C/C++ APIs available since OS/390 R4
  - ►JNDI (Java) LDAP Service provider added in OS/390 R7

- LDAP Server
  - ►available since OS/390 R5
  - ►uses DB2 V5 or V6 tables as backing store
  - ►Sysplex support
  - ►LDAP access to RACF USER and GROUP profiles
  - ►V3 protocol support for OS/390 R8

- Working closely with IETF

Chart 23

LDAP V3 Protocol Support

- Major elements of the LDAP V3 protocol include:
  - ability to obtain support information from server (rootDSE)
  - standardized referral support
  - operational controls
  - ability to bind using a certificate
  - data ’on-the-wire’ in UTF-8 format
  - Does not include schema publication and update

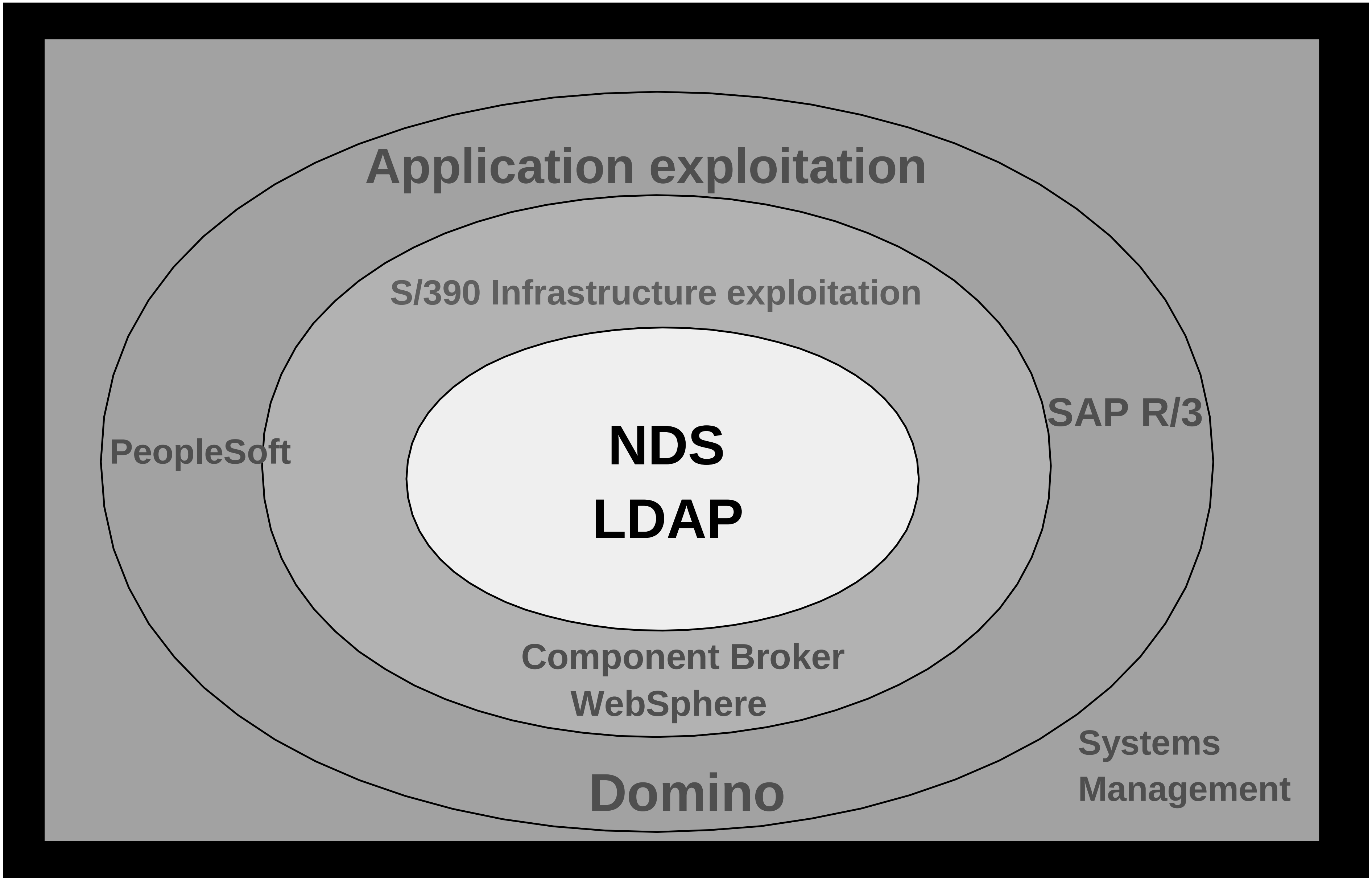
- V3 protocol is invoked in an application by setting the version referenced by the LDAP handle to version 3

Novell NDS on OS/390

- Many customers and vendors committed to NDS
- New NDS releases getting rave reviews
- NDS now available on OS/390
  - Novell Network Services for OS/390
  - OS/390 can be ***the*** **central NDS for the Enterprise**
  - Can consolidate all distributed NDS onto OS/390
  - Includes management and configuration utilities on S/390
  - NDS 5 coming next year
- OS/390 lets customer choose
  - LDAP
  - NDS
  - or both

Chart 25

OS/390 Directory Directions



Application exploitation

S/390 Infrastructure exploitation

SAP R/3

PeopleSoft

NDS
LDAP

Component Broker
WebSphere

Systems
Management

Domino

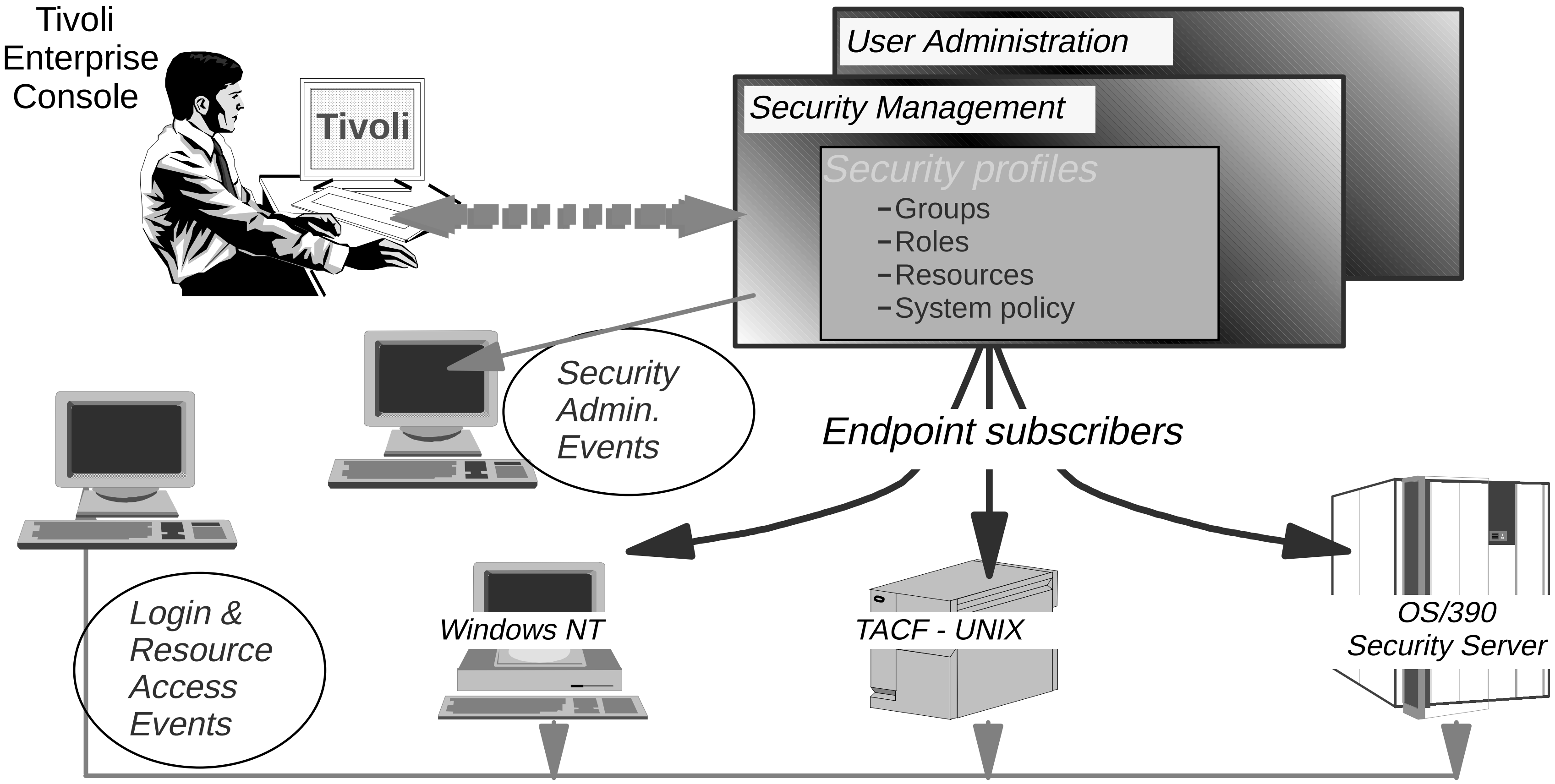
Chart 26

X-Security Model Identity Interoperation

The OS/390 mixed workload environment involves multiple "Security Models". Customers are/will demand X-Security Model Identity Interoperation: Single Signon, and consistent user identity.

- Identity Interoperation between:
  - DCE and RACF (Done OS/390 R1)
  - Digital Certificate (Partly done, OS/390 R4)
  - Future direction:
    - Lotus Notes to RACF
    - Probable need for native Kerberos

Security Administration via Tivoli



As of July 99, available for execution on OS/390

- Tivoli Management Framework
- Tivoli User Administration
- Tivoli Security Management

Chart 28

S/390 Certifications

- E4 (Certification on LPAR). Achieved 1Q99.
- FIPS (Security of the Crypto Co-Processor and 4758).
- ICSA Certification for VPN Cryptographic products 2Q99.

OS/390: Tying It All Together

- Internet Trust Model
  - CDSA - Standard Security/Crypto Interfaces
  - SSL - Popular secure internet communication protocal
  - Crypto - Encrypt data for internet, use Public Key
  - Digital Certificates - Tie back to RACF internet digital certificate
  - PKIX - Implement PKI infrastructure that can communicate cross company
- Consolidated Security for OS/390 Applications
  - Component Broker support, Java Support, Digital Certificate Support
  - NDS/RACF Interoperation, Lotus/RACF Interoperation, Consolidated Security Directory

OS/390: Tying It All Together...

- Enterprise Security Management
  - ►Tivoli support - manage enterprise from one server

- Enterprise Directory
  - ►LDAP - manage enterprise directory from one server
  - ►NDS - manages current enterprise directories

- Peace of mind
  - ►OS/390 Ethical Hacking
  - ►E4 and FIPS Certifications in progress

?

? ?

? ?

? Time for Questions ?

? ?

? ?

?