IBM eServer™

z/OS Security Server Overview

Vanguard Enterprise Security Expo

Reno, Nevada

6 June 2004

Peggy LaBelle
z/OS Security (EIM & RACF) Development and Test
IBM Poughkeepsie
plabelle@us.ibm.com

© 2004 IBM Corporation

Trademarks

- The following are trademarks of International Business Machines Corporation:

  AIX, CICS, DB2, DFSMS, eServer, Hiper Batch, IBM, IMS, iSeries, MVS/ESA, Open Edition, OS/390, OS/400, pSeries, PSF, RACF, VTAM, xSeries, z/OS, zSeries

- The following are trademarks of registered trademarks of other companies or institutions:

  DCE, Distributed Computing Environment,
  NetWare, Novell, NT, Microsoft Corporation,
  Open Software Foundation, Open Software Foundation, Inc., OSF, UNIX

- Other company, product, or service names may be trademarks or service marks of others.

© 2004 IBM Corporation

Disclaimer

The information contained in this document is distributed on an “as is” basis without any warranty either expressed or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in it’s own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM’s licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming, or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

© 2004 IBM Corporation

Table of Contents

© 2004 IBM Corporation

Agenda

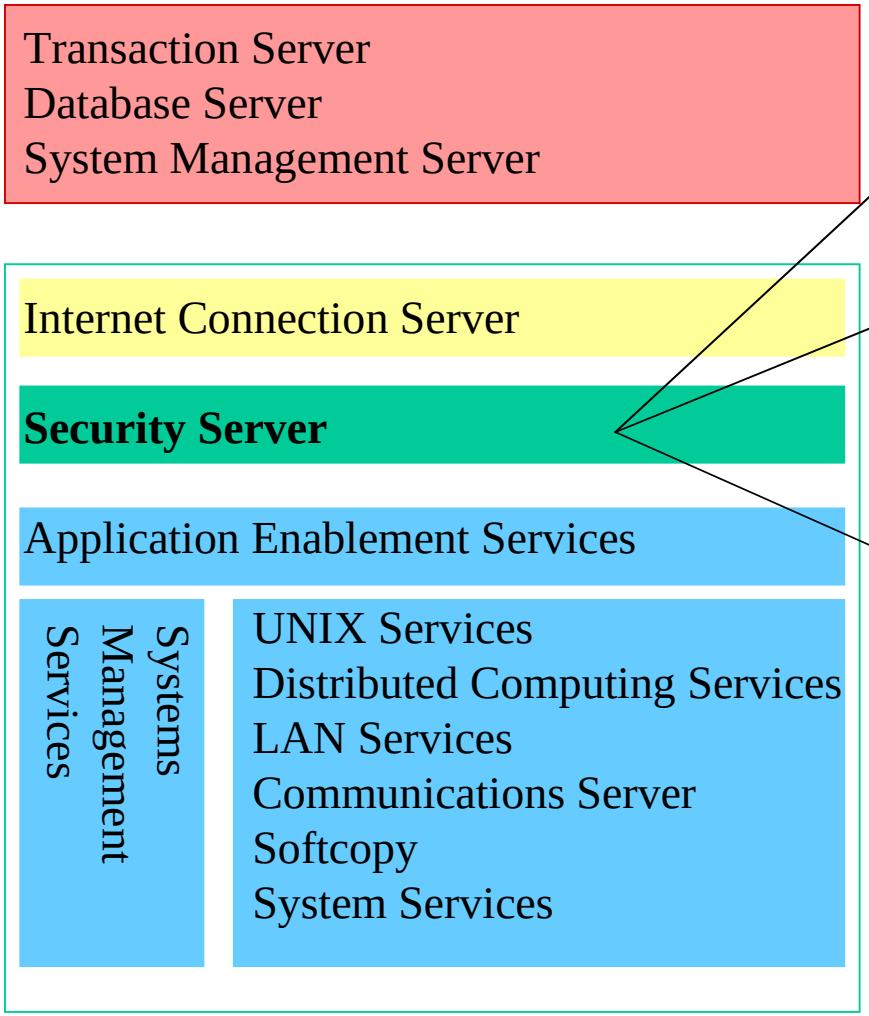
- **Reorganization of the z/OS Security Server in z/OS V1R5**

- **The optional features**
  - **Security Server**
    - RACF

- **The base elements**
  - **Cryptographic Services**
    - ICSF, OCSF, PKI Services, System SSL
  - **Integrated Security Services**
    - DCE, EIM, Firewall Technologies, LDAP,
    - Network Authentication Services (i.e. Kerberos), OCEP

© 2004 IBM Corporation

z/OS Security Server Restructure in z/OS V1R5



z/OS Security Server
- RACF

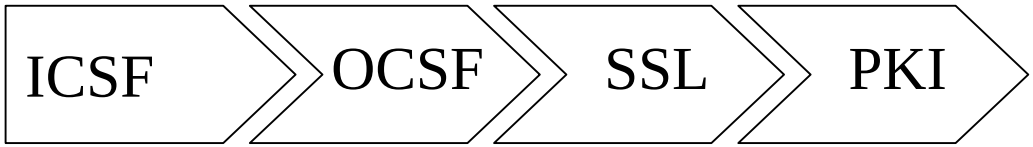
z/OS Cryptographic Services
- ICSF
- OCSF
- PKI Services
- System SSL

z/OS Integrated Security Services
- DCE
- EIM
- Firewall Technologies
- LDAP
- Network Authentication Services
- OCEP

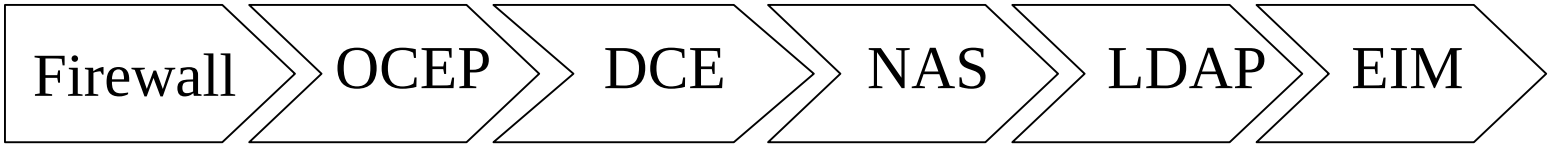
© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services



z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Security Server - RACF

- **RACF – Resource Access Control Facility**
- The RACF element of the z/OS Security Server is a software tool for use by:
  - Security Administrators
  - Auditors
- RACF is used to implement, and monitor the implementation of an installation's security policies
- End user interaction with RACF is minimized by design
- z/OS Resource Managers invoke or call for security services through a set of architected interfaces on z/OS known as the **System Authorization Facility** or **SAF**

© 2004 IBM Corporation

z/OS Security Server - RACF…

User Identification
Authentication

Resource authorization checking
System access control

z/OS Security Server - RACF

Security
Administration

Security console
•Violation reporting

Audit Reports
Integrity Reports

RACF database
• Primary and backup
• Local and remote sharing

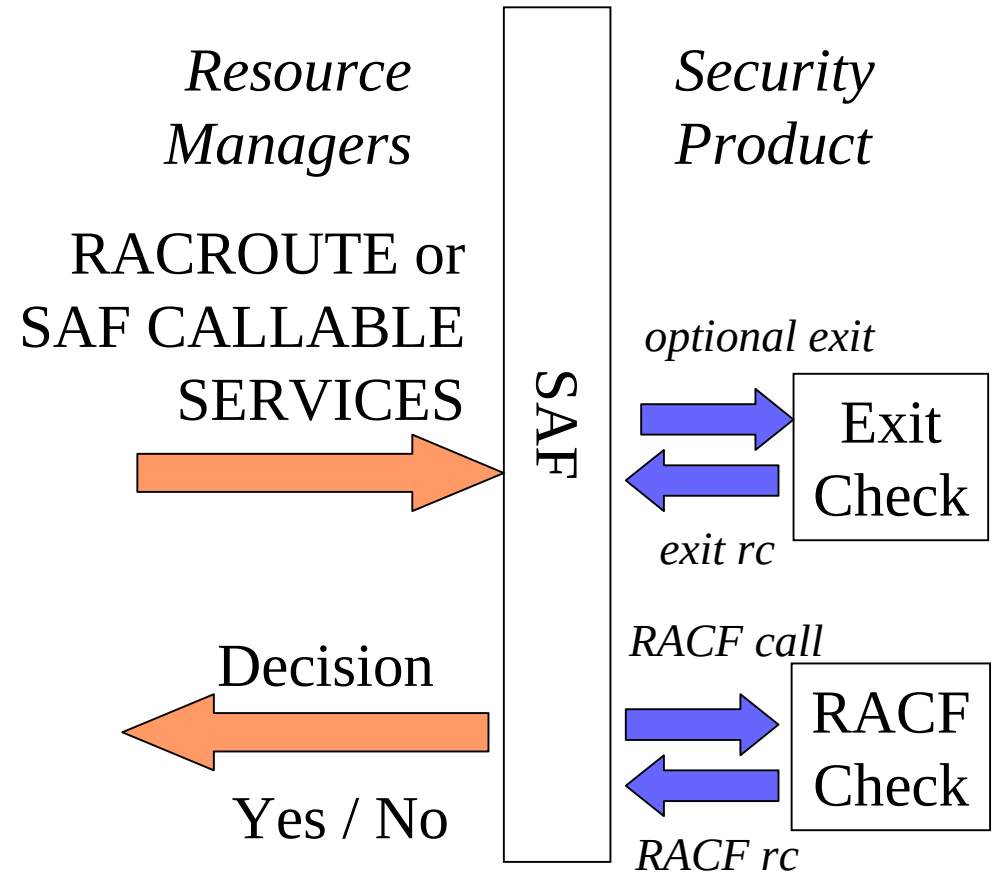
© 2004 IBM Corporation

z/OS Security Server - RACF…

RACF is invoked by resources managers at control points, typically using SAF interfaces.

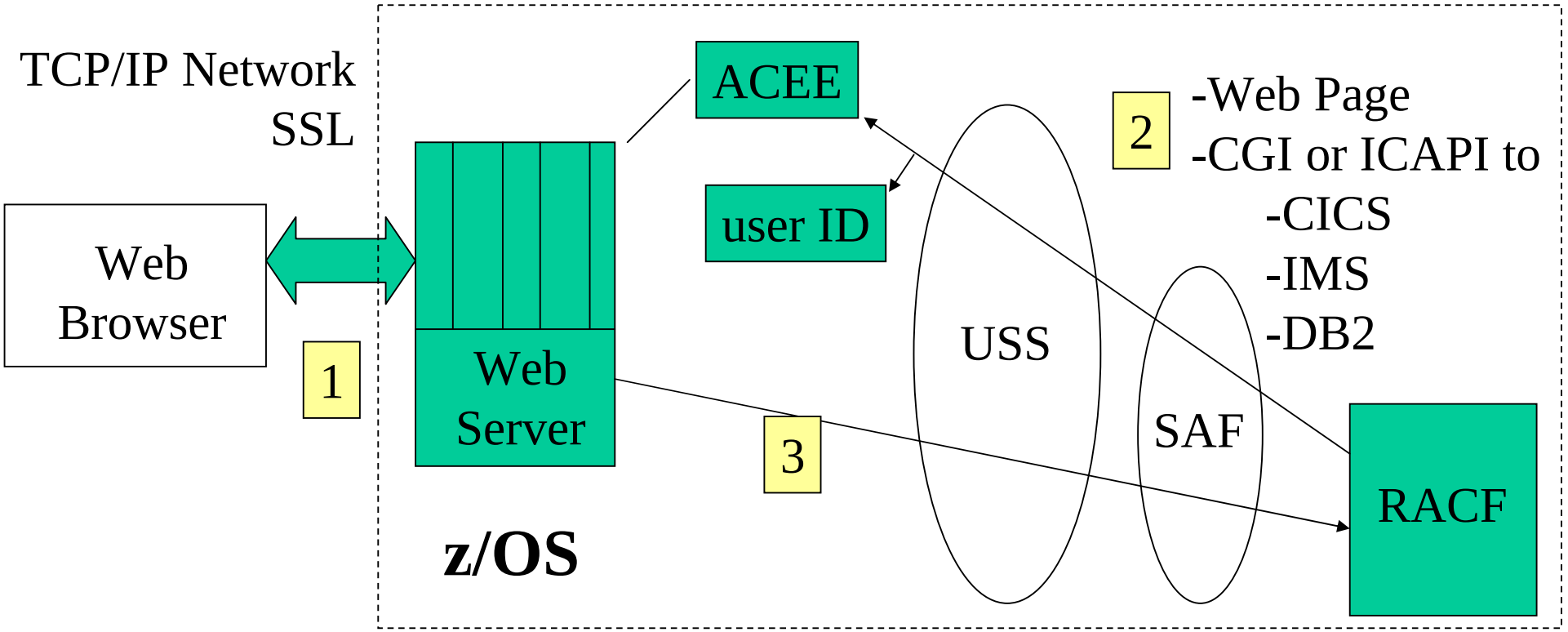
Examples of resource managers:

- UNIX System Services
- Contents Supervisor
- DFP (OPEN, SCRATCH)
- UTILITIES
- Catalog Management
- VSAM
- AMS
- DFSMS
- IMS
- CICS
- TSO
- DB2
- JES2 and JES3
- Console Services
- PSF
- VTAM
- SDSF
- Web sphere
- And more



© 2004 IBM Corporation

z/OS Security Server – RACF and Digital Certs



1. User authenticates to Secured Sockets Layer (SSL)
2. User requests z/OS secured resource via browser
3. Web Server invokes RACF via USS to build local security context (ACEE)

Passing SSL validated certificate instead of prompting for user ID and password!

© 2004 IBM Corporation

z/OS Security Server – RACF

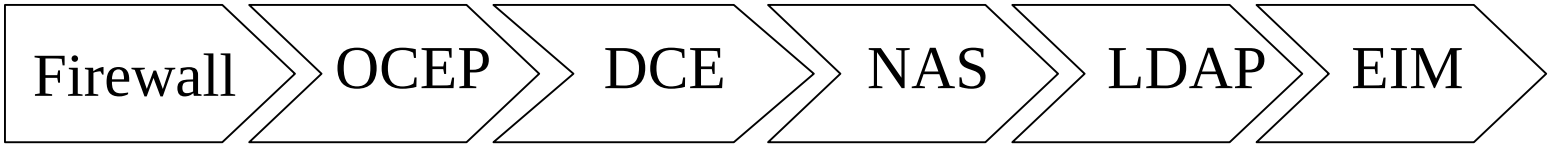
- Digital certificates
  - Introduced in OS/390 R2.4
  - Basis for a complete certificate authority (CA) on z/OS
- Kerberos registry is RACF
- Unix System Services Security integrated with RACF with better security than other UNIX's
- Auditing of security events
- z/OS V1R5
  - Dynamic Templates
  - Multi-level security
  - Password Synchronization Solution
    - RACF, LDAP, and IDI

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Cryptographic Services
Integrated Cryptographic Service Facility(ICSF)

Enciphering
Deciphering
Hashing
Generating digital signatures
Verifying digital signatures

Secret key and
public key cryptography

Callable services
Hardware store
Hardware assists

IBMs Common Cryptographic Architecture (CCA)
- Based on ANSI Data Encryption Algorithm (DEA)
-NIST Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
-Public Key Cryptography Standard (PKCS)
-SET Secure Electronic Transaction standard
-RSA Public key algorithm
-NIST Digital Signature Standard (DSS) algorithm

Keys
DES, triple DES
PINs
MACs
Card Verification Code (CVC)
SET applications
PKA encrypt/decrypt
Europay, MasterCard, Visa(EMV)
Integrated Circuit Card (ICC)

© 2004 IBM Corporation

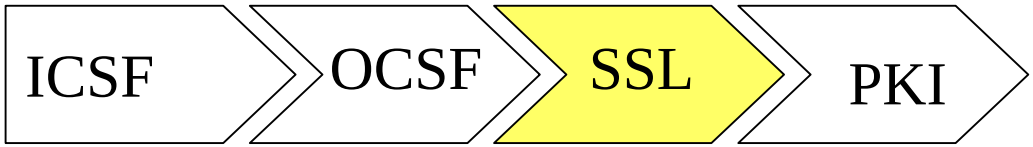
z/OS Cryptographic Services – ICSF

- Designed for high security and high performance
  - Uses DES algorithms
  - Master keys stored in hardware
  - Cryptographic Coprocessors
  - Trusted Key Entry (TKE) workstation (optional)
    - Distributing master and operational keys
  - Callable services for use by applications
    - RACF can control access

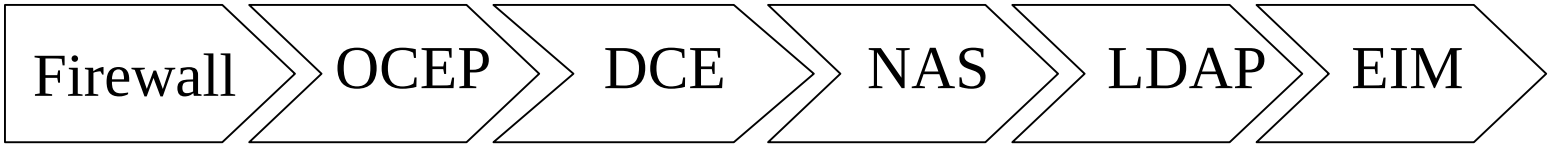
© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services



z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Cryptographic Services – System SSL

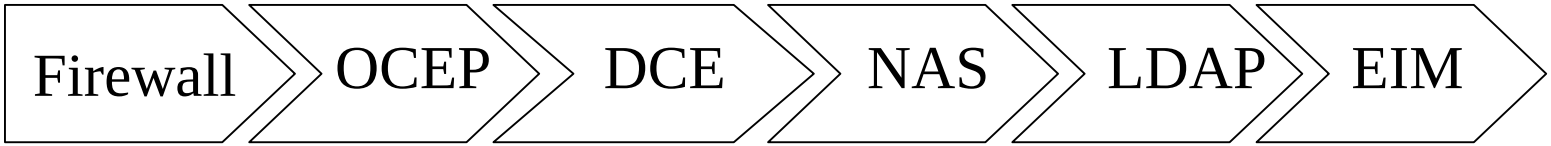
- SSL is a communications protocol for use by two applications communicating over an unsecured network
  - Ensures data privacy and integrity
  - Server and client authentication based on digital certificates
- Essential for secure transactions between web browser and web server
- System SSL gives the option of using RACF digital certificate support

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

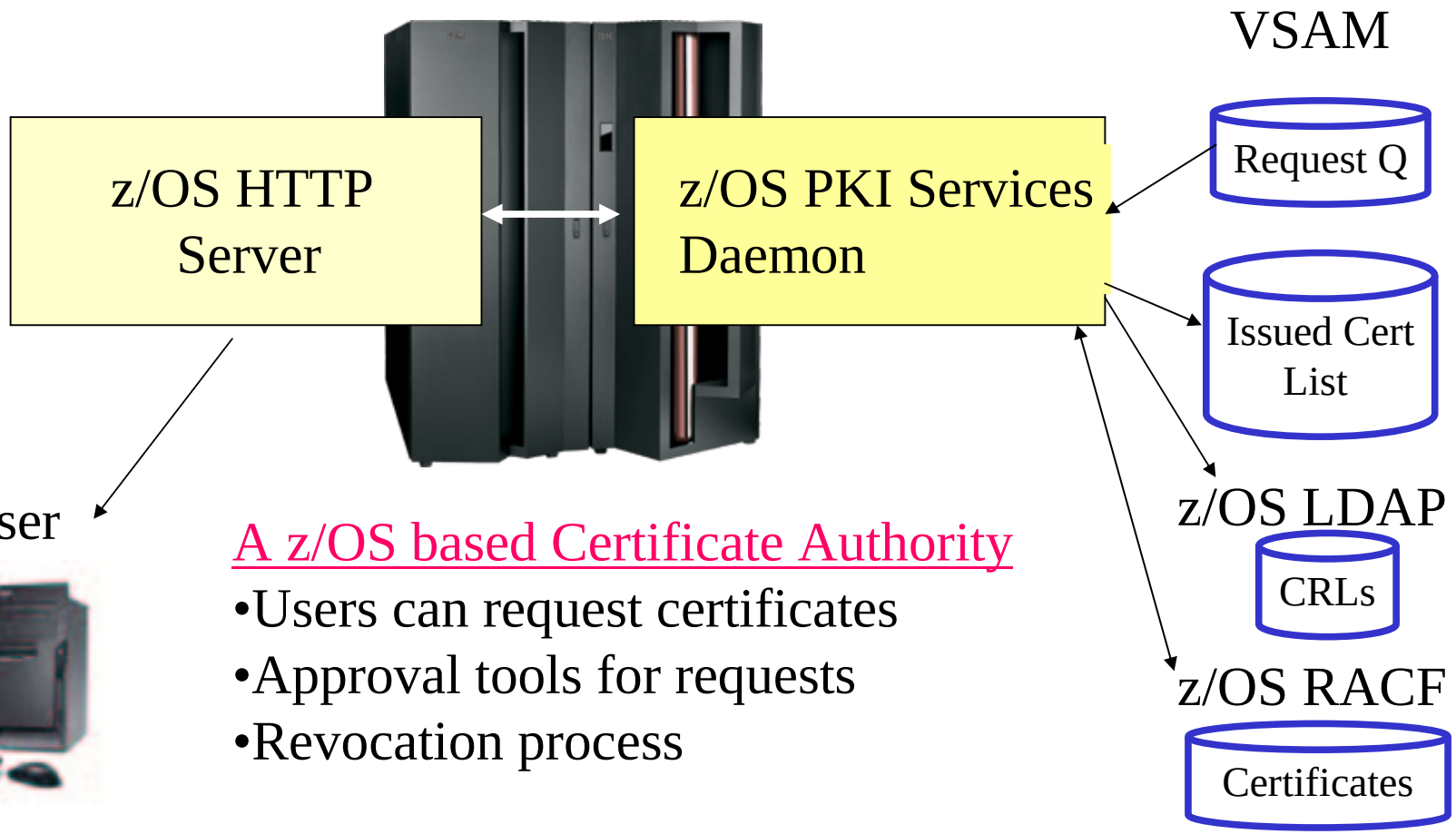
z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Cryptographic Services – PKI Services

PKI – Public Key Infrastructure Services



A z/OS based Certificate Authority

- Users can request certificates
- Approval tools for requests
- Revocation process

© 2004 IBM Corporation

z/OS Cryptographic Services – PKI Services

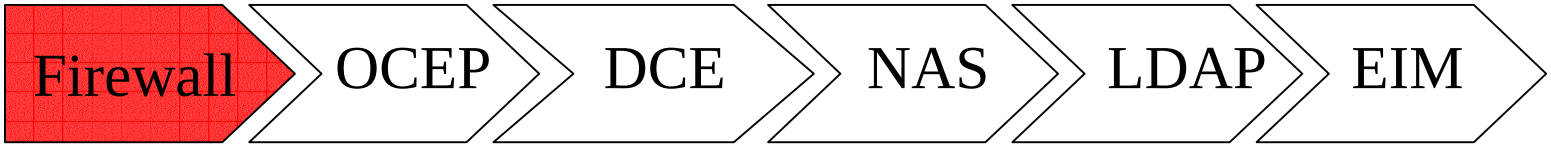
- Public Key Infrastructure (PKI) Services
- Complete certificate authority (CA) package
  - User request driven via customizable web pages
    - Browser or server certificates
  - Automatic or administrator approval process
    - Using same web pages
  - End user / administrator revocation process
- Closely coupled with PKI support in RACF

© 2004 IBM Corporation

z/OS Security Server

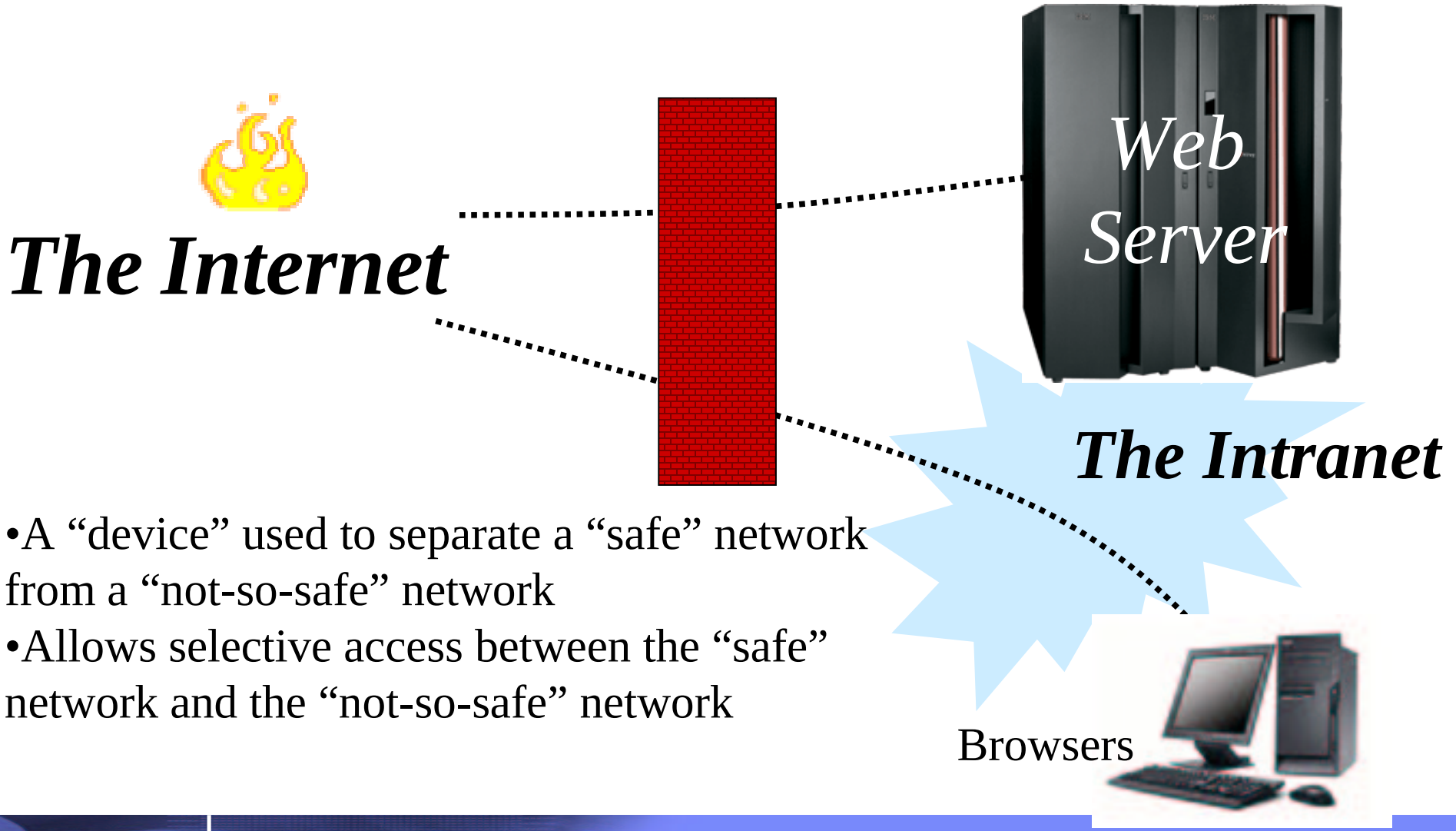
z/OS Cryptographic Services

z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Integrated Security Services – Firewall



- A “device” used to separate a “safe” network from a “not-so-safe” network
- Allows selective access between the “safe” network and the “not-so-safe” network

© 2004 IBM Corporation

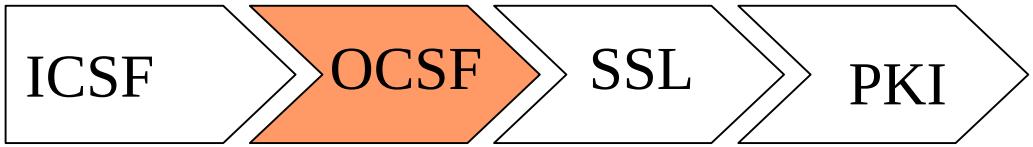
z/OS Integrated Security Services – Firewall Technologies

- Access Control
  - IP Packet Filter
  - FTP (Application Gateway) Proxy
  - SOCKS (Circuit Gateway) Server
  - Network Address Translation (NAT)
  - Virtual Private Networks (VPN)
  - Internet Key Exchange (Dynamic VPN)
- Management Logs and Reports
  - Monitor and Detect
  - Administration GUI

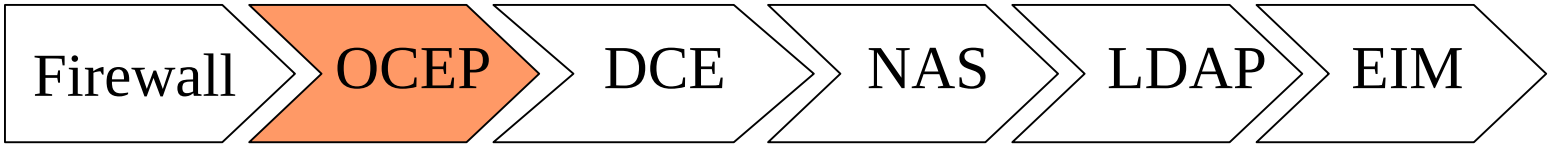
© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services



z/OS Integrated Security Services

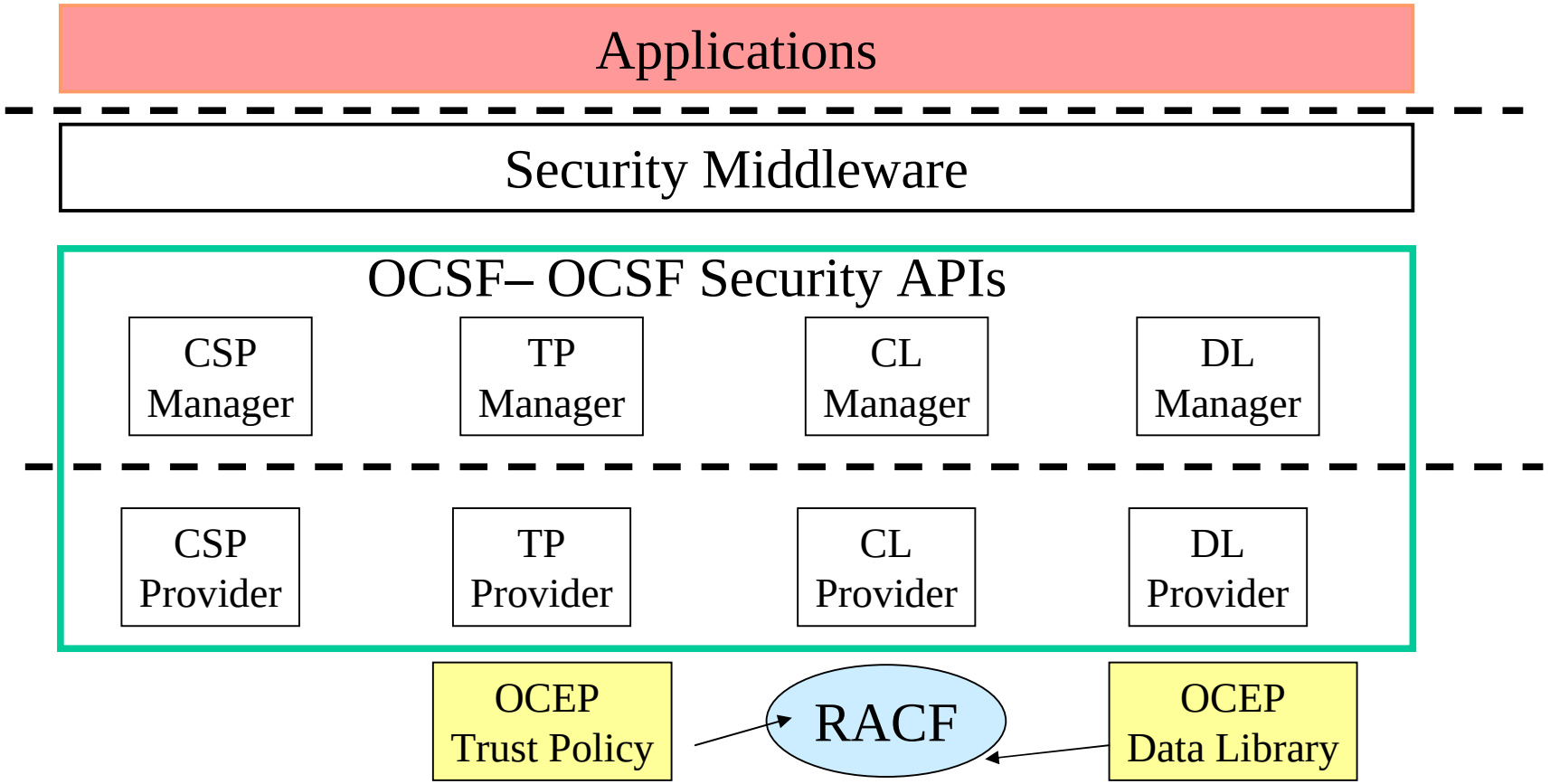


© 2004 IBM Corporation

z/OS Integrated Security Services - OCEP

OCSF – Open Cryptographic Services Framework

OCEP – Open Cryptographic Enhanced Plug-in



© 2004 IBM Corporation

z/OS Integrated Security Services - OCEP

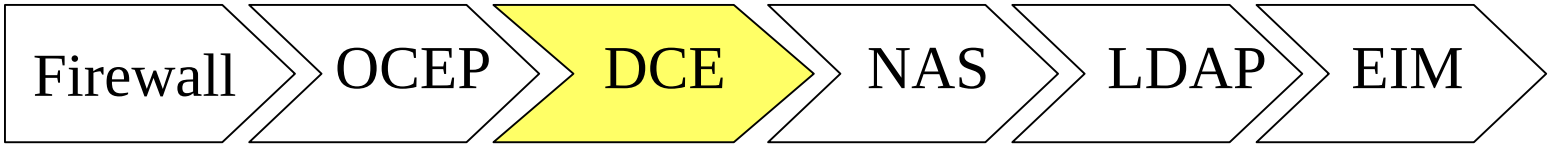
- OCSF
  - Common Data Security Architecture (CDSA)
    - IBM/Intel Security framework; X/Open Group standard
  - Unix APIs to utilize certificates and keys
- OCEP
  - Data Library Plug-In provides “read-only” access to RACF key rings
  - Trust Policy Plug-In verifies trustworthiness of a RACF key ring
    - Checks key rings
    - Certificates marked TRUST in RACF
- Solutions: Firewall, System SSL

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

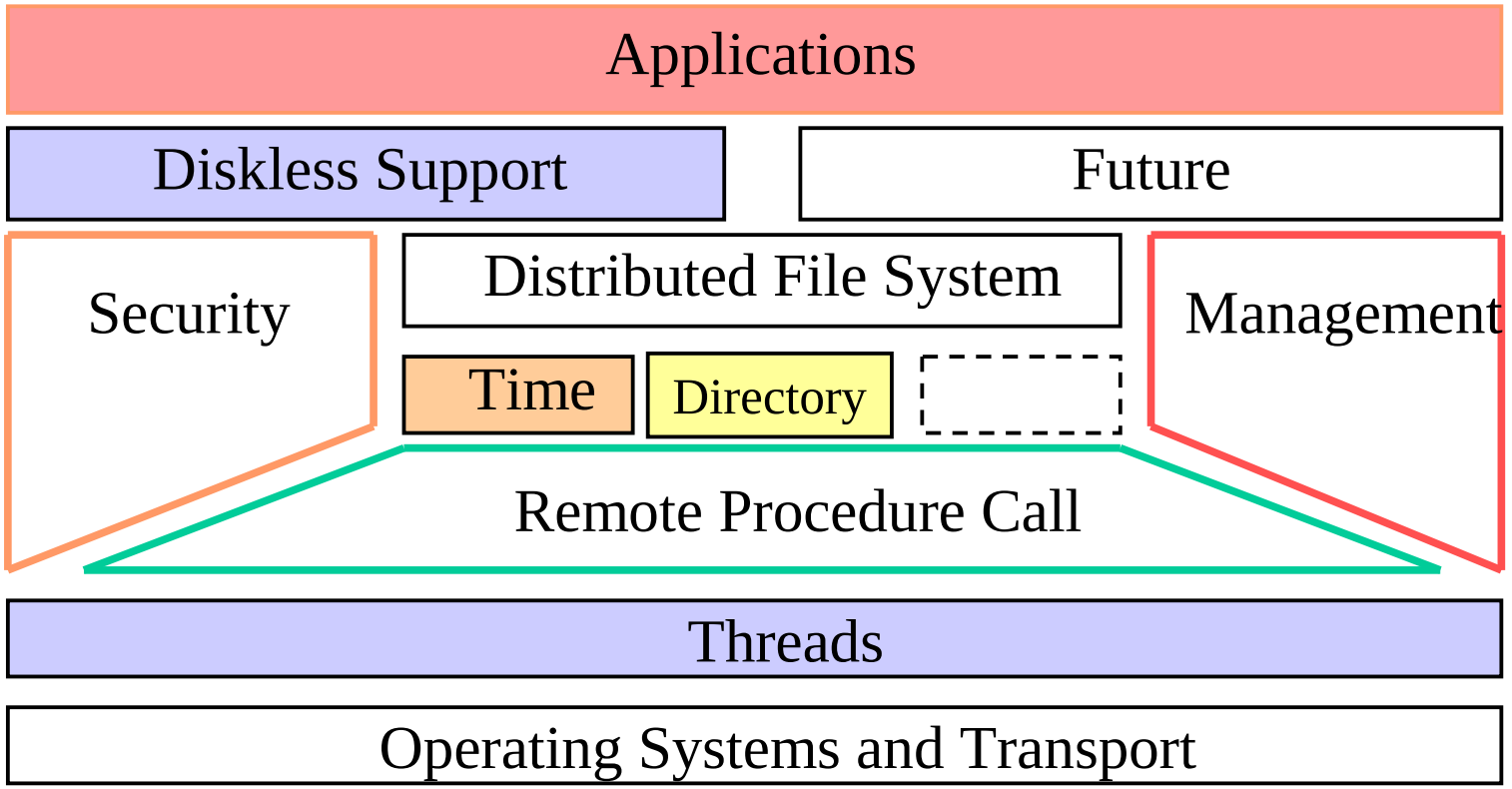
z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Integrated Security Services - DCE

DCE – Distributed Computing Environment



© 2004 IBM Corporation

z/OS Integrated Security Services - DCE

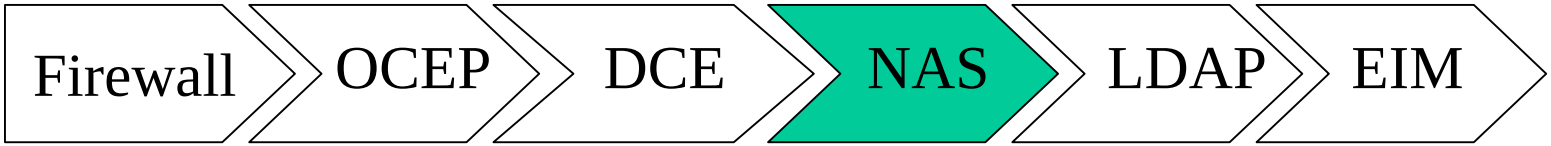
- Provides self contained environment and tools for developing and running applications on heterogeneous distributed systems
  - Remote Procedure Calls (RPCs)
  - Directory
  - Time
  - Security – Kerberos (not part of base)
  - Threading
- C++ not supported
- Supported by IBM, HP, SUN, DEC, Hitachi, others.

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Integrated Security Services - NAS

NAS – Network Authentication Services

Kerberos (Cerberus) was the mythological three-headed dog that guarded the entrance to the underworld. Unless you could get past Kerberos, you could not enter (or leave!) the underworld).

© 2004 IBM Corporation

z/OS Integrated Security Services – Network Authentication Services (NAS)

realm

Key Distribution Center (KDC)

Authentication Server

Ticket Granting Server

AS
- Authenticates Users
- Grants TGTs

TGS
- Generates Session Keys
- Grants Service tickets based on TGTs

Ethel

RACF

Kerberos Registry

Realm A

© 2004 IBM Corporation

z/OS Integrated Security Services - NAS

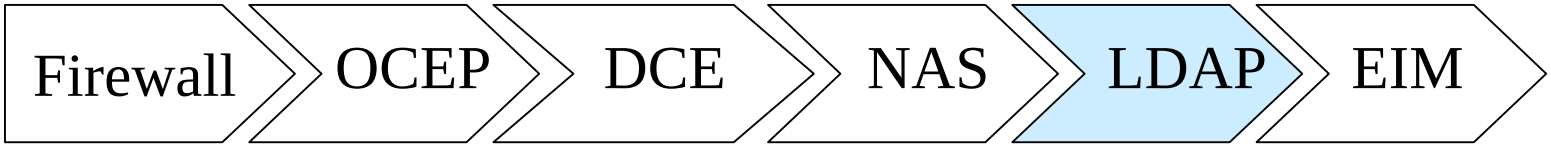
- **Kerberos allows authentication over physically untrusted network**
  - Depends on a trusted third party – the KDC
- **Kerberos on z/OS**
  - Kerberos registry is integrated into RACF registry
  - Behaves like any other Kerberos “Realm”
  - Realm to realm function supported
  - Standards
    - RFC 1510 – Kerberos V5
    - RFC 1964 – GSS-API
- **Users**
  - Network based applications based on Kerberos authentication
  - IBM DB2 V7 and Web sphere V4

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

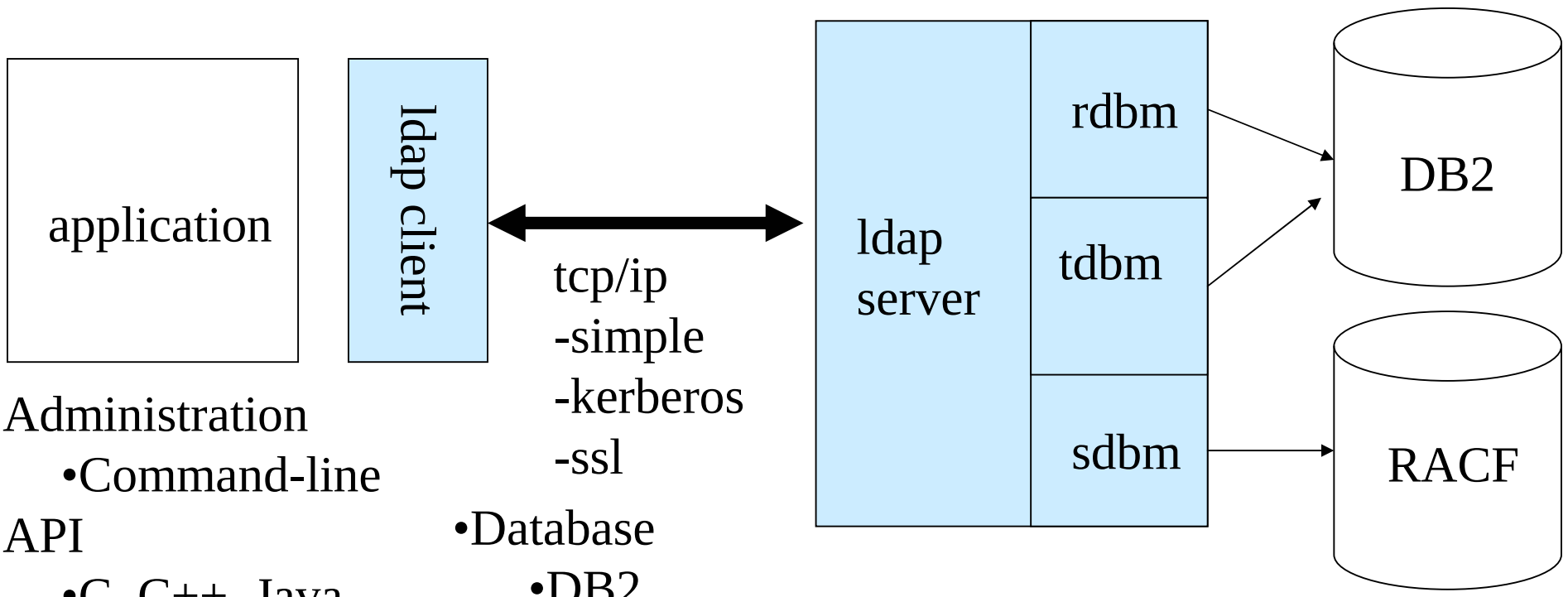
z/OS Integrated Security Services



© 2004 IBM Corporation

z/OS Integrated Security Services - LDAP

LDAP – Lightweight Directory Access Protocol



- Administration
  - Command-line
- API
  - C, C++, Java
- Protocol
  - LDAP V2 and V3
- Database
  - DB2
- Schema
  - Many elements common to other directories

© 2004 IBM Corporation

z/OS Integrated Security Services - LDAP

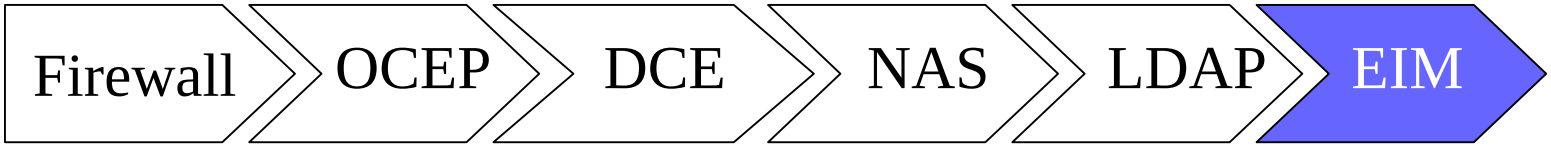
- What is a Directory Service?
  - A database that holds phone-book, location, configuration information
  - Optimized for frequent reads, infrequent updates
  - Based on IETF x.509 standards
- IBM Directory Products
  - z/OS Integrated Security Services LDAP
  - IBM Directory Server
  - IBM Tivoli Directory Server
  - Client APIs and Servers

© 2004 IBM Corporation

z/OS Security Server

z/OS Cryptographic Services

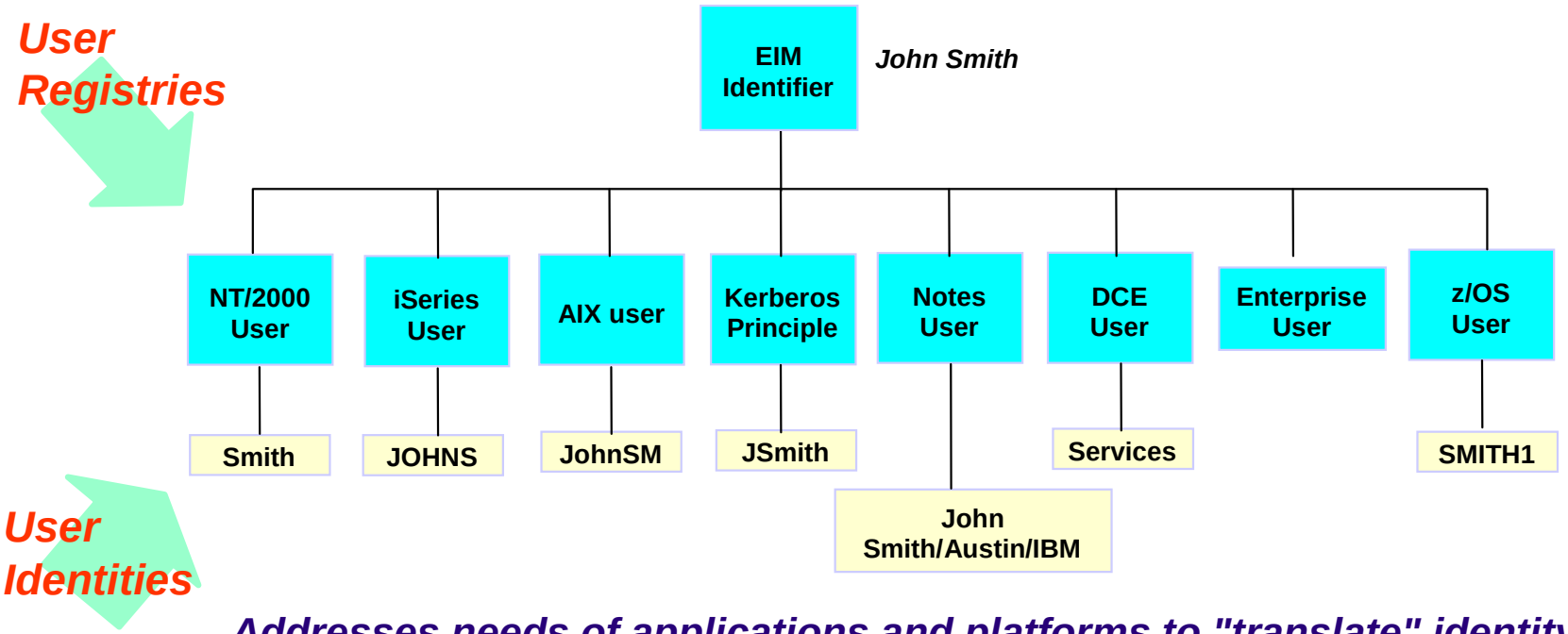
z/OS Integrated Security Services



© 2004 IBM Corporation

Enterprise Identity Mapping

- **EIM defines** associations between an identifier and user ids in registries that are part of OS platforms, applications, and middle-ware.
- The identity associations (*mappings*) are stored in a well known location, e.g. LDAP, with common services across platforms to access the mappings.



Addresses needs of applications and platforms to "translate" identity when crossing platform and registry boundaries.

© 2004 IBM Corporation

z/OS Integrated Security Services - EIM

- Addresses needs of applications and platforms to "translate" identity when crossing platform and registry boundaries.
- Middleware infrastructure
- Available on iSeries, pSeries, xSeries, zSeries
- Complementary to Tivoli Identity Manager

© 2004 IBM Corporation

Session Summary

The optional features

Security Server

RACF

The base elements

Cryptographic Services

ICSF, OCSF, PKI Services, System SSL

Integrated Security Services

DCE, EIM, Firewall Technologies, LDAP,
Network Authentication Services (i.e. Kerberos), OCEP

© 2004 IBM Corporation