Welcome To The ITSO Workshop
z/OS V1R9 z Security Update

Redbooks
International Technical Support Organization

1. z/OS Security status as of z/OS V1R8 - z/OS V1R9 preview
2. z/OS Security Server at z/OS V1R9
3. z/OS remote Security services
4. Tivoli zSecure overview
5. System z hardware cryptography status review
6. z/OS support of the PKCS#11 cryptographic API
7. RACF keyrings and PKI Services updates
8. z/OS System SSL updates
9. z/OS Network Authentication Service update
10. z/OS Communications Server Security updates

z/OS Security Technologies
Where We Stand at z/OS V1R8
z/OS V1R9 Preview

Session
01

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

z Security Update

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- z/OS Security Services and APIs
- z/OS Cryptographic Services
- z/OS Security Server
- z/OS Integrated Security Services
- Java APIs for z/OS Security services
- z/OS LDAP status
- z/OS Communications Server Security services
- OpenSSH for z/OS

Revised And Expanded Statement Of z/OS Integrity

IBM z/OS V1.9 Announcement Letter, August 7, 2007

First issued in 1973, IBM's MVS™ System Integrity Statement and subsequent statements for IBM OS/390® and z/OS have stood for three decades as a symbol of IBM's confidence in and commitment to the z/OS operating system. Today, IBM reaffirms its commitment to z/OS System Integrity.

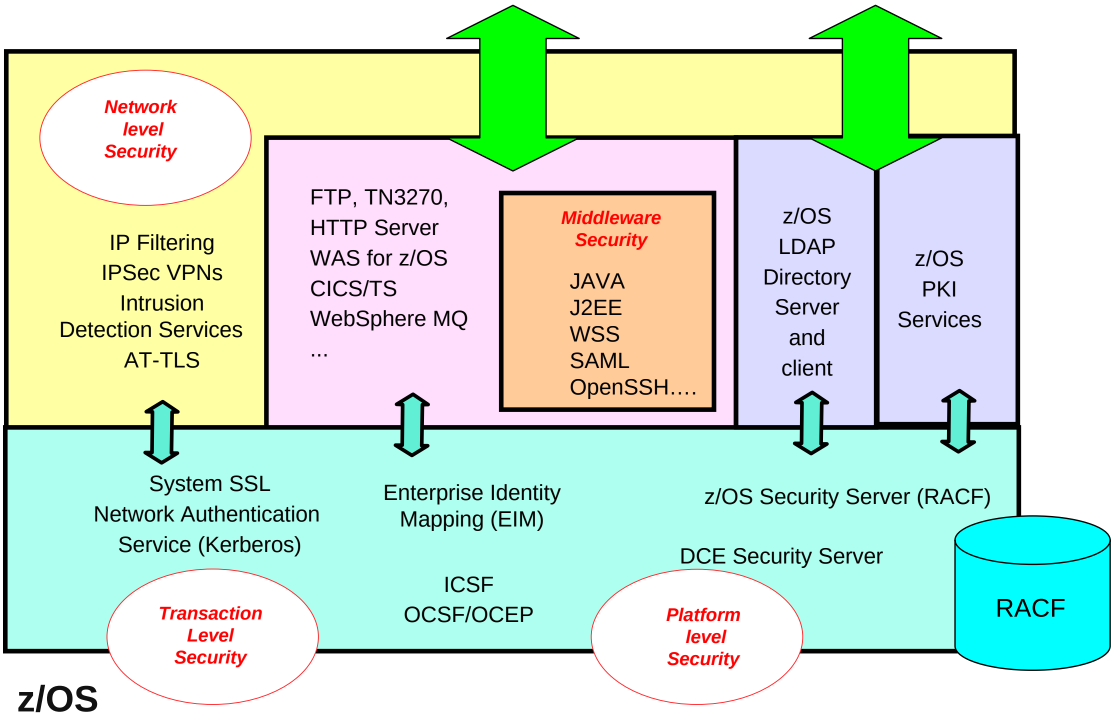
IBM's commitment includes designs and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security — that is, to prevent them from gaining access to, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation.

Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than 8, or Authorized Program Facility (APF) authorized.

In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

z/OS Security Services and APIs

z/OS Security Services And APIs



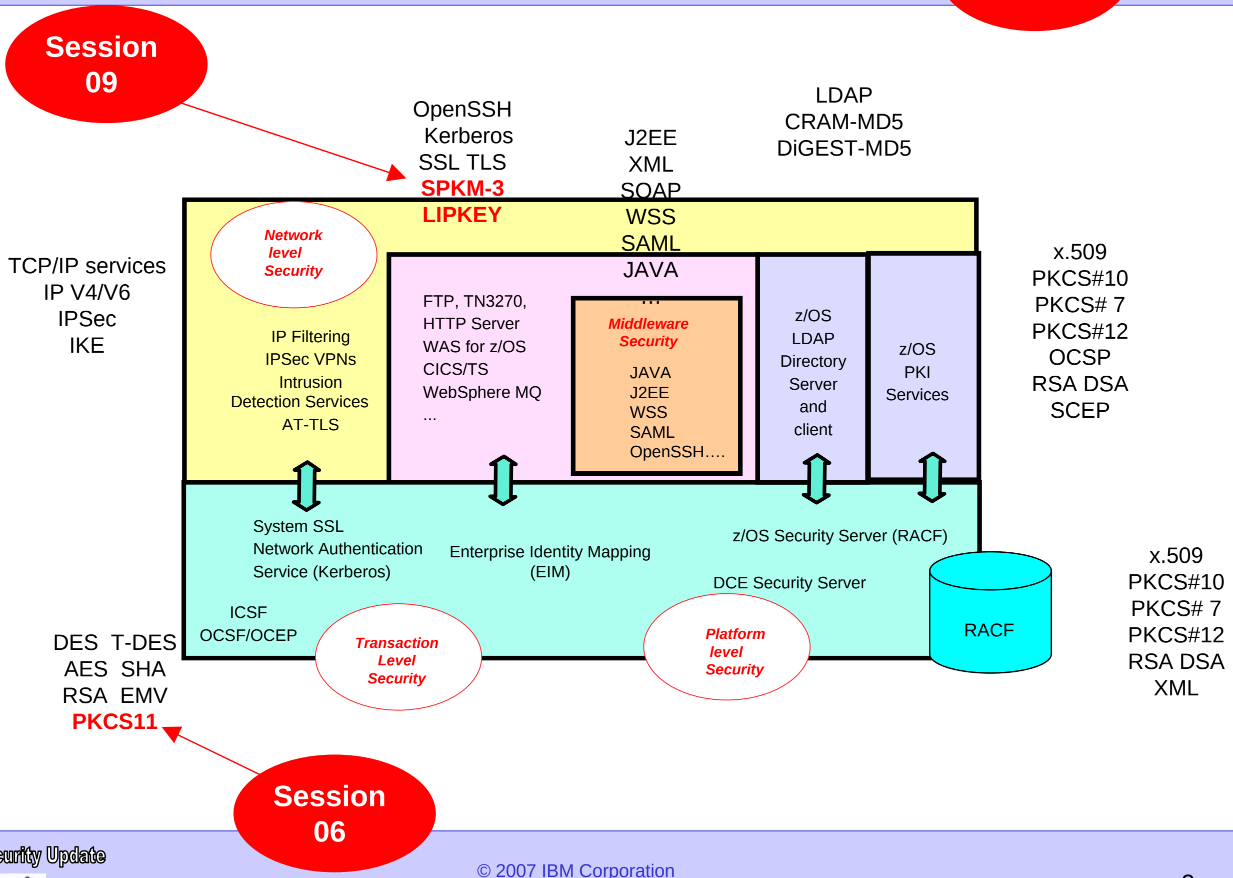
z/OS Security Services And APIs - Packaging

Changes at z/OS V1R9

z/OS Cryptographic Services	ICSF OCSF System SSL PKI Services pkitp	(Integrated Cryptographic Service Facility) (Open Cryptographic Services Facility) (Secure Socket Layer) (Public Key Infrastructure Services) (PKI Trust Policy)
z/OS Security Server	RACF (* license required)	(Resource Access Control facility)
z/OS Integrated Security Services	ISS LDAP Directory Server DCE Security Server OCEP Network Authentication Service Enterprise Identity Mapping (EIM) Remote Services - Identity Cache	(Lightweight Directory Access Protocol) (Distributed Environment Computing) (Open Cryptography Enhanced Plug-in) New at R8/R9
IBM Tivoli Directory Server for z/OS (ITDS)	LDAP server and client	
Communications Server	IP Security: IPSec, IP Filtering Intrusion Detection Services AT-TLS	(Application Transparent TLS)
z/OS Java APIs	See the dedicated slides	New API at R9
IBM Ported Tools For z/OS (5655-M23): OpenSSH For z/OS	unpriced feature – z/OS Implementation of the OpenSSH protocol and services for Unix System Services users	

z/OS Security Services – Supported Standards

New at z/OS V1R9



z/OS Security Services – Cryptography Export Controls

Security Level 3 FMIDs

Unpriced features, worldwide exportable subject to U.S. export regulations
Required to have the z/OS security services performing encryption with > 64-bit keys

z/OS V1.R9 Communications Server Security Level 3
FMID JIP619K

See details in
“z/OS Planning for Installations “, GA22-7504.

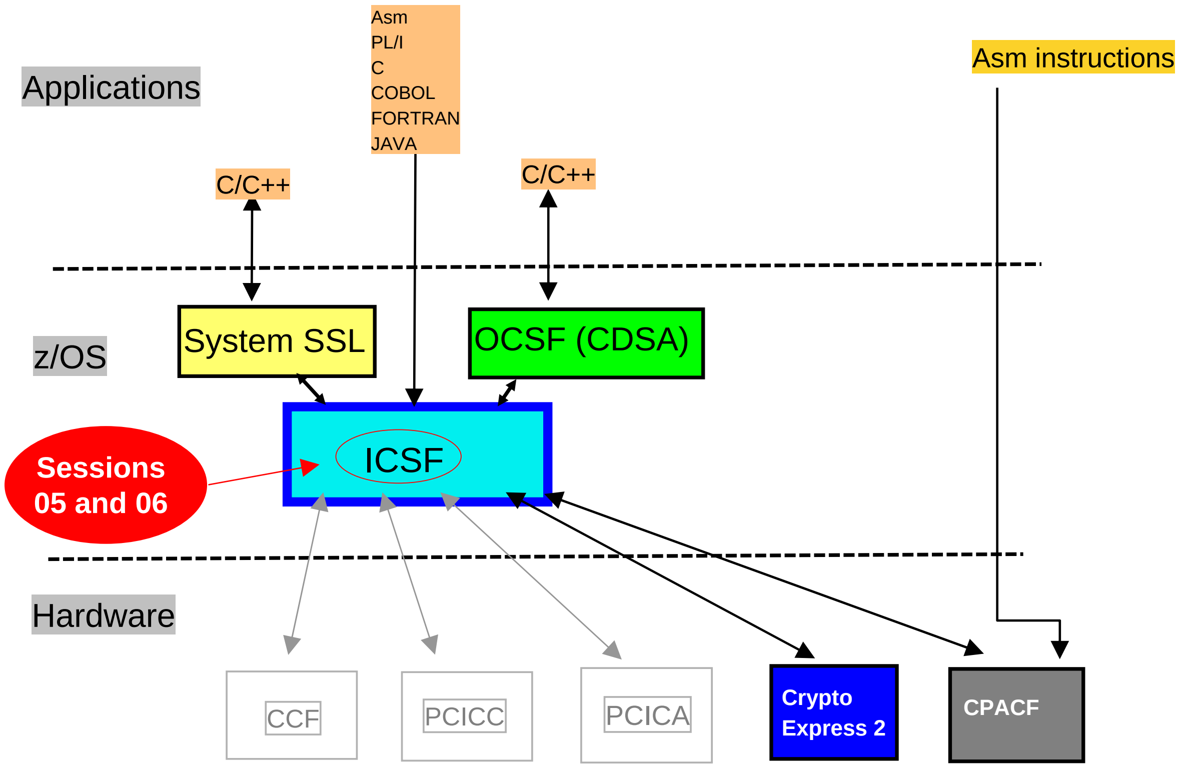
z/OS V1.R9 Security Level 3 contains
FMIDs JCPT391 JCRY741 JRSL381 JSWK391

- Tivoli Directory Server for z/OS Security Level 3 includes ISS LDAP Server Level 3
- OCSF Security Level 3
- Network Authentication Service Level 3
- System SSL Security Level 3

Java cryptography is controlled with the default policy files
The unrestricted policy files have to be downloaded:
http://www-03.ibm.com/servers/eserver/zseries/software/java/j5jcecca.html

z/OS Cryptographic Services

z/OS Cryptographic Services



z/OS Open Cryptographic Service Facility

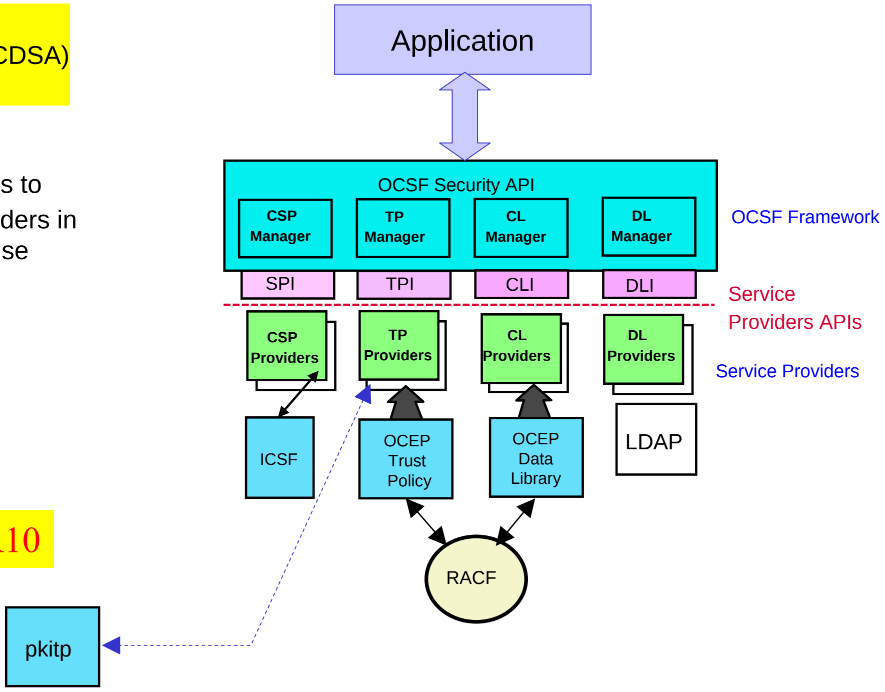
OS/390 implementation of
Common Data Security Architecture (CDSA)
Intel/IBM Security framework

Provides a set of open security services to support applications and protocol providers in a context of Public Key Infrastructure use

CSP = Cryptographic Services Provider
TP = Trust Policy
CL = Certificate Library
DL = Data Library
SPI = Service Provider Interface
OCEP = Open Cryptographic Enhanced Plug-in

Last changed in OS/390 V2R10

The pkitp (pki trust policy) plugin is shipped since z/OS V1R3



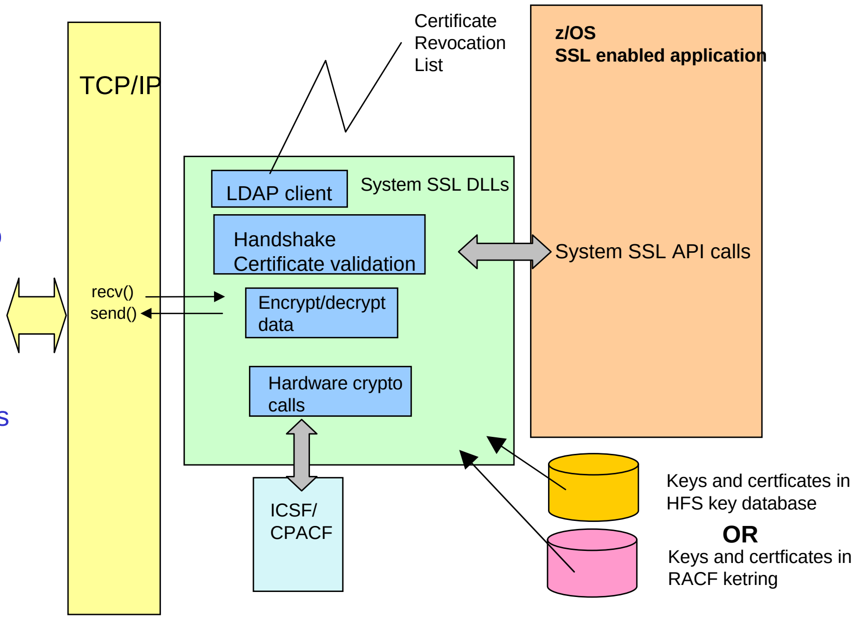
z/OS System SSL

- A set of C/C++ functions for establishing and using SSL/TLS socket connections as an SSL/TLS server or client

- A set of C/C++ functions for applications to
  - manipulate keys and certificates databases
  - exploit keys and certificates stored in databases
  - build and process PKCS#7 messages

- A key and certificates management facility (GSKKYMAN)

Sessions 06 and 08

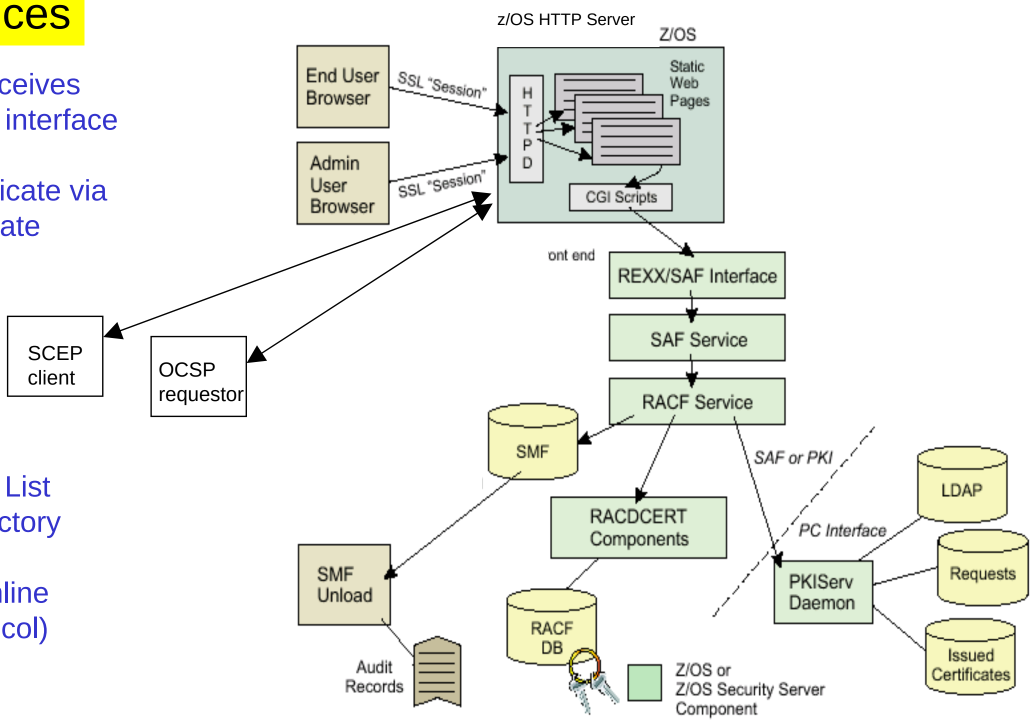

TCP/IP
recv()
send()
Certificate Revocation List
z/OS SSL enabled application
LDAP client
System SSL DLLs
Handshake Certificate validation
System SSL API calls
Encrypt/decrypt data
Hardware crypto calls
ICSF/ CPACF
Keys and certficates in HFS key database
OR
Keys and certficates in RACF ketring

SSL=Secure Socket Layer
TLS= Transport Layer Security

z/OS Cryptographic Services

z/OS PKI Services

- User requests and receives certificate via browser interface
- Client can get a certificate via SCEP (Simple Certificate Enrolment Protocol)



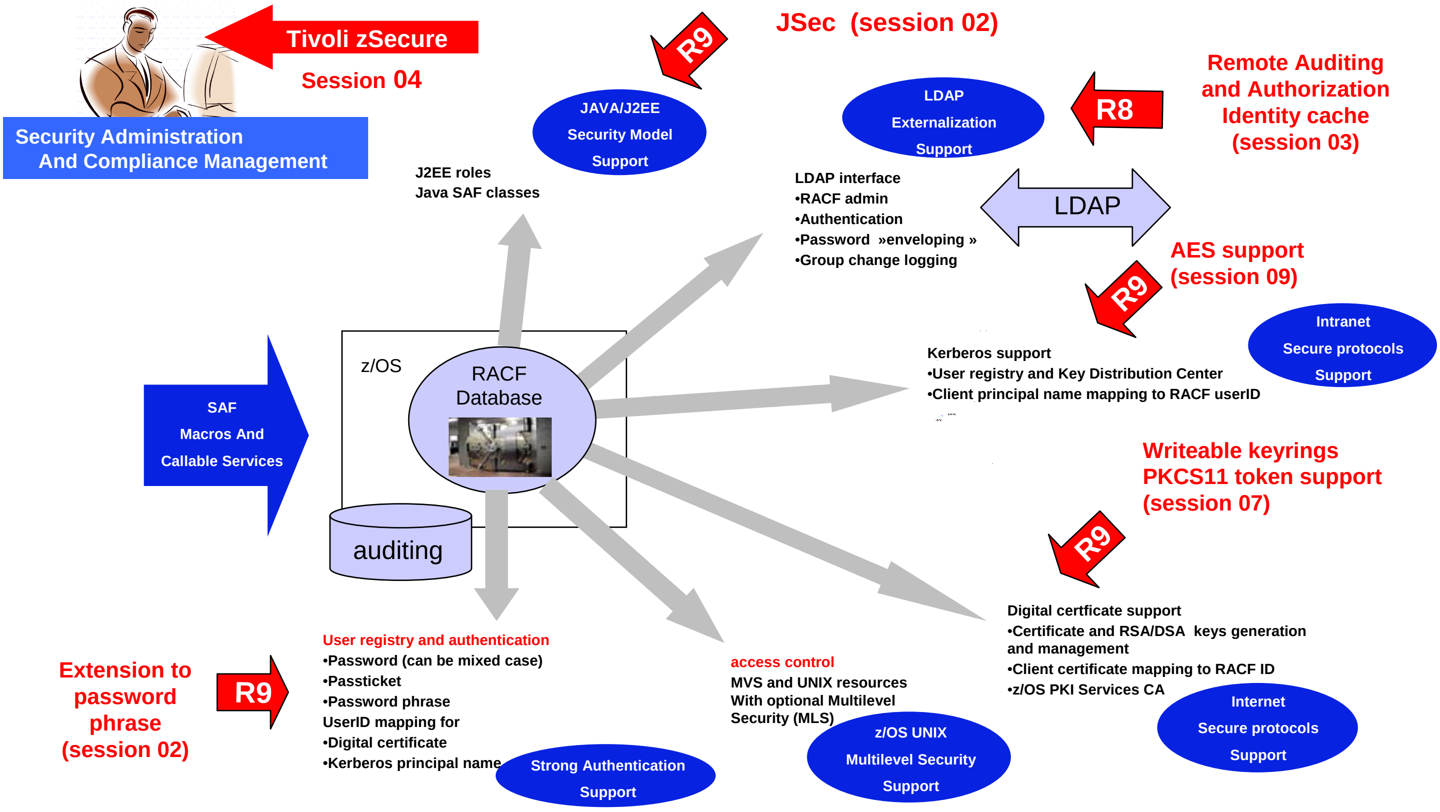
- Certificate Revocation List published in LDAP directory and HTTP files
- Support for OCSP (Online Certificate Status Protocol)

Session 07

Identrus compliant

z/OS Security Server

z/OS Security Server - RACF



Tivoli zSecure

Session 04

Security Administration
And Compliance Management

R9

JSec (session 02)

JAVA/J2EE
Security Model
Support

J2EE roles
Java SAF classes

LDAP
Externalization
Support

R8

Remote Auditing
and Authorization
Identity cache
(session 03)

LDAP interface
- RACF admin
- Authentication
- Password »enveloping »
- Group change logging

LDAP

R9

AES support
(session 09)

Intranet
Secure protocols
Support

Kerberos support
- User registry and Key Distribution Center
- Client principal name mapping to RACF userID

SAF
Macros And
Callable Services

z/OS

RACF
Database

auditing

Writeable keyrings
PKCS11 token support
(session 07)

R9

Digital certficate support
- Certificate and RSA/DSA keys generation and management
- Client certificate mapping to RACF ID
- z/OS PKI Services CA

Internet
Secure protocols
Support

Extension to
password
phrase
(session 02)

R9

User registry and authentication
- Password (can be mixed case)
- Passticket
- Password phrase

UserID mapping for
- Digital certificate
- Kerberos principal name

Strong Authentication
Support

access control

MVS and UNIX resources
With optional Multilevel
Security (MLS)

z/OS UNIX
Multilevel Security
Support

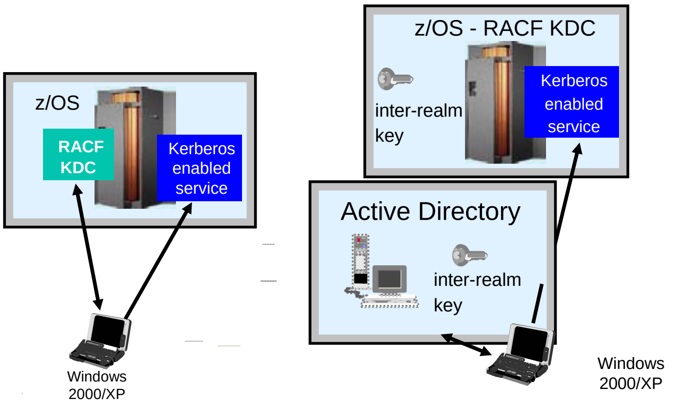
z/OS Integrated Security Services

z/OS Network Authentication Service

Kerberos support for z/OS KDC or applications

Kerberos-enabled z/OS servers

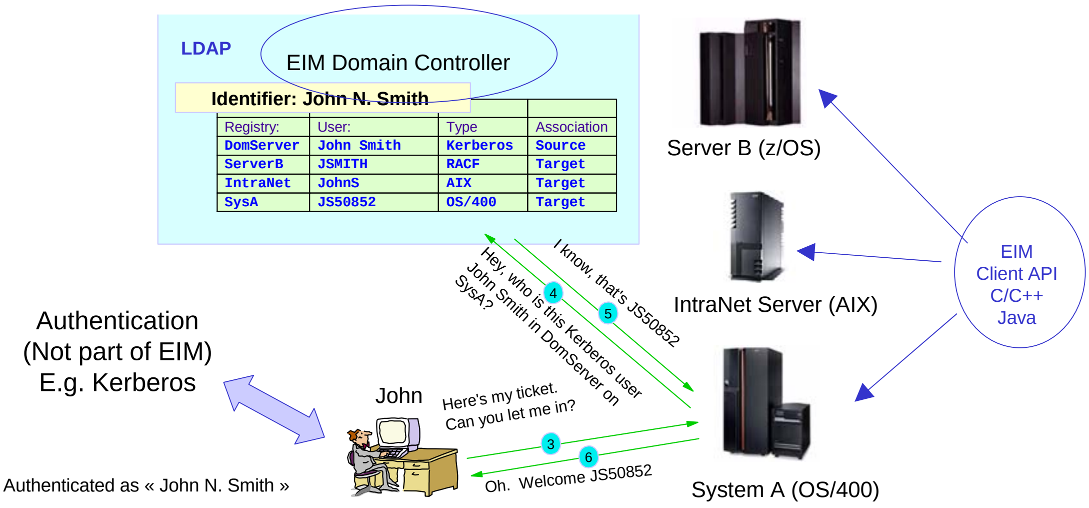
- •**DB2** V7 and above (authentication)
- •**WebSphere Application Server** (authentication)
- •**FTP** client and server (authentication, optional encryption)
- •**Telnet server** (authentication, optional encryption)
- •**LDAP** client and server (authentication)
- •**rshd** server (authentication, optional encryption)



Session 09

Addition of the SPKM-3/LIPKEY protocols support

Enterprise Identity Mapping (EIM)


LDAP
EIM Domain Controller
Identifier: John N. Smith
Server B (z/OS)
IntraNet Server (AIX)
System A (OS/400)
EIM Client API C/C++ Java
Authentication (Not part of EIM) E.g. Kerberos
John
Authenticated as « John N. Smith »
Here's my ticket. Can you let me in?
3
Hey, who is this Kerberos user John Smith in DomServer on SysA?
4
I know, that's JS50852
5
6
Oh. Welcome JS50852

Registry:	User:	Type	Association
DomServer	John Smith	Kerberos	Source
ServerB	JSMITH	RACF	Target
IntraNet	JohnS	AIX	Target
SysA	JS50852	OS/400	Target

Proposed as an identity mapping default mechanism for z/OS applications/middlewares (e.g. in DB2 V9)

The new remote services and ICTX component in z/OS V1R8/R9 are packaged with EIM

Session 03

Java APIs For z/OS Security Services

z/OS Security Services – Java APIs

APIs provided in z/OS

- RACF Passticket Java evaluation and generation (z/OS V1R7)
  /usr/include/java_classes/IRRRacf.jar & IRRRacfDoc.jar

- EIM Java client (z/OS V1R7)
  /usr/lpp/eim/lib/

- RACF users and groups administration – JSec

See Session 02

APIs provided in the IBM SDK for z/OS

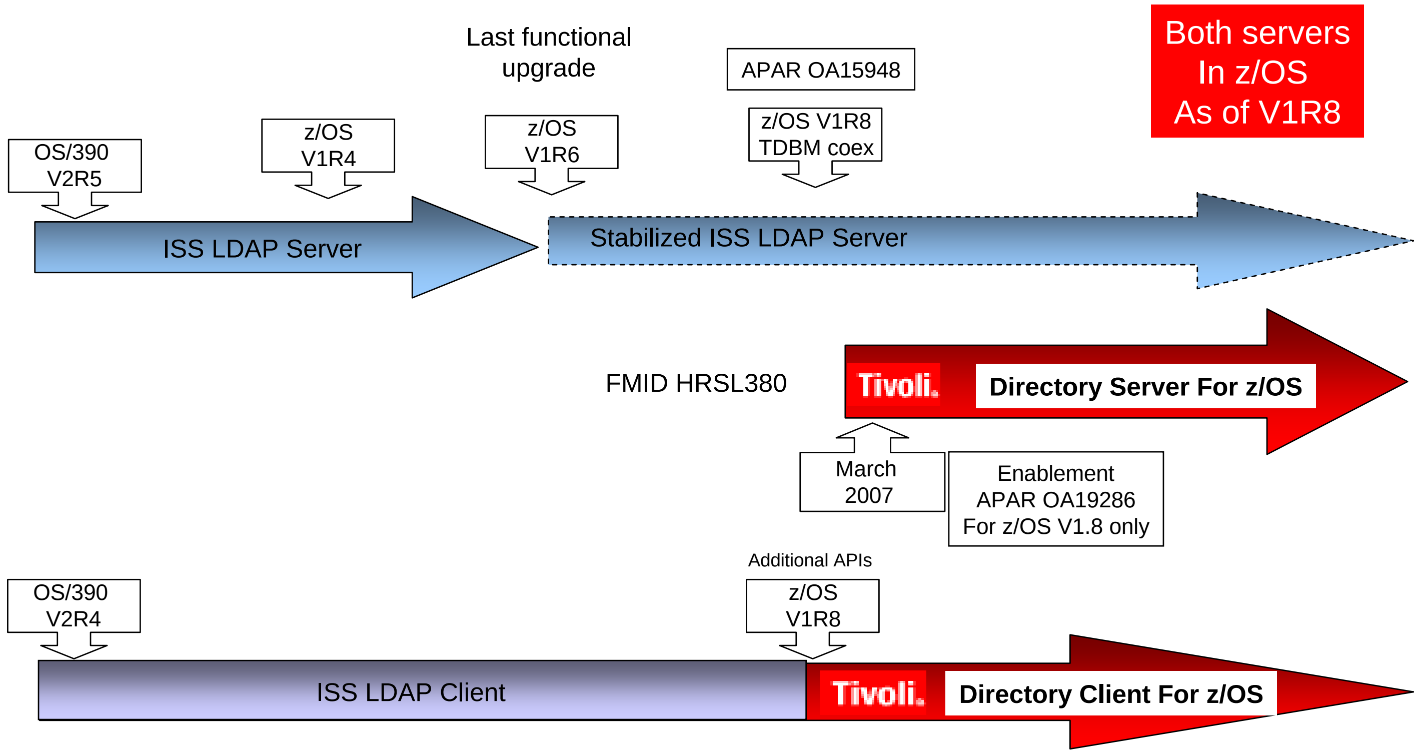
SAF classes (JDK V1.R4): PlatformAccessControl, PlatformThread, PlatformSecurityServer, PlatformAccessLevel, PlatformReturned, PlatformUser

See the appendix for further details

z/OS LDAP

A Status

ITDS For z/OS – The Whole Story Revealed …



Last functional upgrade

APAR OA15948

Both servers In z/OS As of V1R8

OS/390 V2R5

z/OS V1R4

z/OS V1R6

z/OS V1R8 TDBM coex

ISS LDAP Server

Stabilized ISS LDAP Server

FMID HRSL380

Tivoli. Directory Server For z/OS

March 2007

Enablement APAR OA19286 For z/OS V1.8 only

Additional APIs

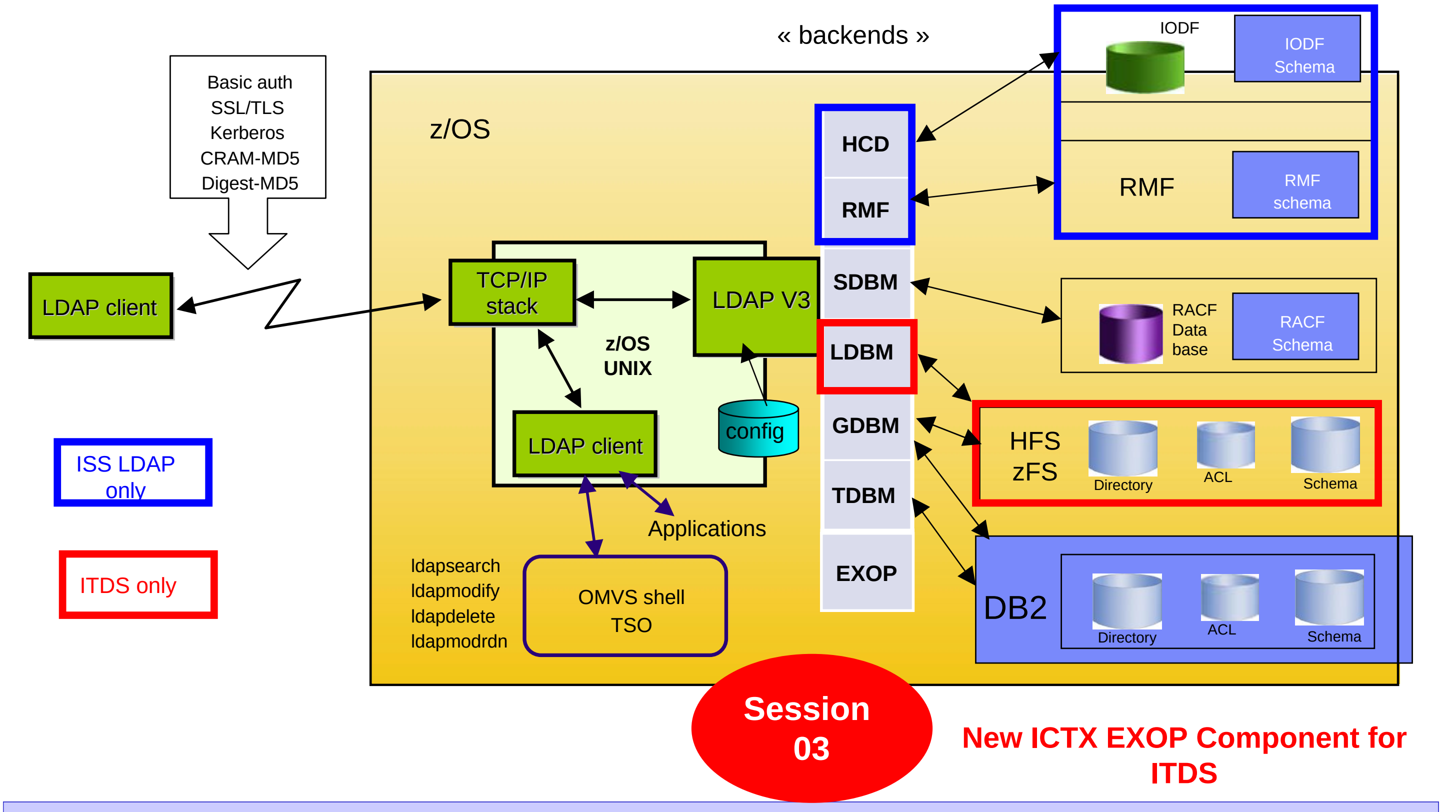
OS/390 V2R4

z/OS V1R8

ISS LDAP Client

Tivoli. Directory Client For z/OS

z/OS V1R8 LDAP - ISS LDAP And ITDS



New ICTX EXOP Component for ITDS

A Very Quick Overview Of z/OS Communications Server Security Services

Session 10

z/OS Communications Server At z/OS V1R8

Not any more « Firewall Technologies »

- Replaced by « IP Security Services »
  - IP Filtering (static filters)
  - IPSec Virtual Private Networks
    - •DES, T-DES, AES128, SHA-1, MD5
    - •IKE, RSA
    - •NAT Traversal RFCs (RFC 3947/3948)

Application-Transparent TLS (AT-TLS)

- SSL/TLS performed by the TCP/IP stack on behalf of the application

Intrusion Detection Services (IDS)

- Host based network IDS
- Scanning and attacks detection, traffic regulation

Additional Unpriced Product

-

OpenSSH For z/OS

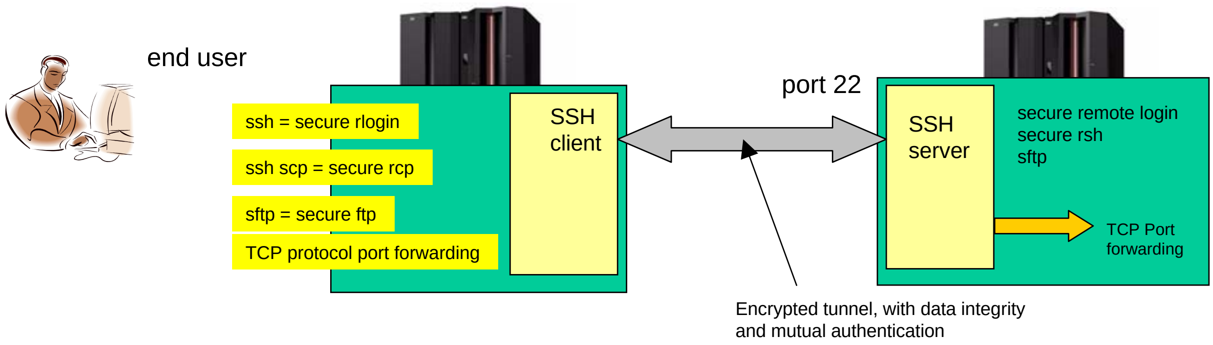
OpenSSH For z/OS

OpenSSH – suite of network connectivity tools that provide secure encrypted communications between two untrusted hosts over an insecure network.

Program product: IBM Ported Tools for z/OS (5655-M23) - unpriced, runs on z/OS 1.4 or higher.

Use the SSH protocol for
- Secure remote login (ssh)
- Secure copy program (scp)
- Secure FTP (sftp)

With a « TCP Port Forwarding » capability



end user

ssh = secure rlogin

ssh scp = secure rcp

sftp = secure ftp

TCP protocol port forwarding

SSH client

port 22

SSH server

secure remote login
secure rsh
sftp

TCP Port forwarding

Encrypted tunnel, with data integrity and mutual authentication

Thank You

Any Questions ?

Appendix

Bibliography

- /www.ibm.com/security
- ITSO : Stay Coll on OS/390 : Installing Firewall Technologies - SG24-2046
- ITSO : S/390 Cryptography - SG24-5455
- ITSO : S/390 PCI Crypto Coprocessor SG24-5942
- ITSO : zSeries Crypto Update SG24-6870
- ITSO : z990 Crypto SG24-7070
- ITSO : Ready for ebusiness: OS/390 Security Server Enhancements SG24-5158
- ITSO : OS/390 Security Server 1999 Update SG24-5629, SG24-5627
- ITSO : Putting the Latest z/OS Security Features to work SG24-6540
- ITSO : Implementing VPNs in a z/OS Environment SG24-6530
- ITSO : z/OS TCPIP Security SG24-5383
- ITSO : z/OS 1.6 Security Update SG24-6448
- ITSO : z9 Crypto and TKE V5.0 Update SG24-7123 (in preparation)
- ITSO : z/OS R7 Sysplex Security SG24-7150
- ITSO : Encryption Facility for z/OS SG24-7318
- ITSO : Encryption Facility for z/OS – OpenPGP Support SG24-7434

- z/OS Security Server LDAP
  - SC24-5923 : Server Administration and Usage Guide
- UNIX System Services
  - GA22-7800 : UNIX System Services Planning
- MLS
  - GA22-7509 : Planning for MultiLevel Security and Common Criteria
- EIM
  - SA22-7875 : Integrated Security Services EIM Reference
- PDAS
  - SC24-6040 : PDAS for z/OS Customization and Use
- z/OS Firewall Technologies
  - SC24-5922 : FW Technologies Guide and Reference
- z/OS Open Cryptographic Services Facility
  - SC24-5899 : OCSF Developer's Guide and Reference
- z/OS System SSL
  - SC24-5901 : System SSL Programming Guide and Reference
- z/OS Network Authentication Services (Kerberos)
  - z/OS Security Server Network Authentication Service Administration - SC24-5926

- z/OS PKI Services
  - SA22-7693 : Cryptographic Services PKI Services Guide and Reference
- z/OS Communications Server
  - z/OS Communications Server IP Configuration Guide , SC31-8775
  - z/OS Communications Server IP Configuration Reference, SC31-8776
- IBM Tivoli Directory Server for z/OS
  - SC23-5191 IBM Tivoli Directory Server (ITDS) Server Administration and Use for z/OS
  - SA23-2214 IBM Tivoli Directory Server (ITDS) Client Programming for z/OS

ICSF

SA22-7519	z/OS ICSF Overview
SA22-7520	z/OS ICSF System Programmer's Guide
SA22-7522	z/OS ICSF Application Programmer's Guide
SA22-7521	z/OS ICSF Administrator's Guide
SA22-7523	z/OS ICSF Messages
SA23-2211	ICSFTrusted Key Entry PCIX Workstation User’s Guide
SB10-7036	PR/SM Planning Guide