OS/390 and z/OS Security Server

RACF Update

Mark Nelson
RACF Development
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601l
(845) 435-7758
markan@us.ibm.com

SHARE
Session 1732
July 2001

Disclaimer

The information contained in this document is distributed on an "as is" basis without any warranty either express 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 customers using the information or techniques will obtain the same or similar results in their own operational environments.

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 environments.

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.

Trademarks

- **The following are trademarks or registered trademarks of the International Business Machines Corporation:**
  - IBM, CICS, DB2, z/OS, OS/390, RACF, SecureWay, S/390
- **UNIX is a registered trademark of The Open Group in the United States and other countries.**
- **Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.**
- **Other company, product, and service names may be trademarks or service marks of others.**

Agenda

- **RACF's digital certificate support for OS/390 Version 2 Release 4 and Version 2 Release 6**
- **OS/390 Version 2 Release 8**
  - Digital certificate support
  - Protected user IDs
- **OS/390 Version 2 Release 9**
  - Certificate name filtering
  - Restricted user IDs

Agenda...

- **OS/390 Version 2 Release 10**
  - Security Server enhancements
    - RACF:
      - ✓ Digital certificate support enhancements
      - ✓ PKIServe web-based certificate authority
      - ✓ Program control usability enhancement
      - ✓ Application identity mapping
      - ✓ Mixed case profiles
      - ✓ DB2 Version 7 support
    - Network Authentication Service
      - ✓ New OS/390 Security Server component
      - ✓ Provides Kerberos V5 support
    - LDAP Server enhancements
  - Communications Server enhancements
    - TN3270
    - SERVAUTH controls

Agenda...

- **z/OS Release 2 Enhancements**
  - Security Server
    - RACF:
      - ✓ UNIVERSAL groups
      - ✓ SAF Trace
      - ✓ Cross-system VLF
      - ✓ Coupling Facility error toleration
    - Network Authentication Service
      - ✓ New encryption methods
      - ✓ New client commands
      - ✓ Additional exploiters
  - Communications server
    - Express Logon
    - Network authentication
    - Intrusion detection
    - FTP

RACF's Support for Digital Certificates

RACF's Certificate Support

- What is a digital certificate?
  - Data token which contains a public key, user information, and an endorsement of the validity of the certificate
  - Basis for the distribution of public keys
  - Certificate endorsement is done by Certificate Authorities
  - Certificate validation is done using public key technology
  - Certificates are managed by users
  - Can be used as the basis for user identification and authentication

RACF's Certificate Support

- **OS/390 Release 4**
  - RACF an be used to map certificates to a RACF user ID
    - Certificate is loaded into the RACF database
    - Mapping is based on the issuer's distinguished name and the serial number of the certificate
    - New General resource class **DIGTCERT**
    - RACF command **RACDCERT** to manage the certificates
- **OS/390 Release 6**
  - Certificate self-registration (APARs OW31933, OW33091)
  - Usability enhancements to RACDCERT

Release 8

RACF's Certificate Support...

- **OS/390 Release 8**
  - Enhancements to the RACDCERT command:
    - Generation of certificates for OS/390-based servers
    - Generation of certificates and certificate requests
    - Definition of certificate authority (CERTAUTH) and site (SITE) certificates.
    - Aggregation of certificates into RACF-managed key rings
    - Importation of PKCS-12 certificates
    - Renaming of the LABEL that is associated with a certificate
  - New General resource class **DIGTRING**
  - New "anchor" user IDs: irrcerta and irrsitec

Protected User IDs

- **Allows a user to be defined to RACF that :**
  - May NOT be used to logon to TSO, sign on to CICS, or rlogin from a workstation
  - No signons that need a password
- **Protects user IDs assigned to OS/390 UNIX, UNIX daemons and other important started tasks and subsystems :**
  - From being used for other unintended purposes
  - From being REVOKED for invalid password attempts
  - Helps prevent these IDs from being misused if administrator forgets to change password from a default group value
- **Implemented through the use of NOPASSWORD keyword on ADDUSER and ALTUSER**

RACF's Certificate Support...

- **OS/390 Release 9 "Timeframe"**
  - Certificate Name Filtering: Maps certificates to user IDs based on the content of the certificate
    - Subject's distinguished name
    - Issuer's distinguished name
    - System information (e.g. SMF ID, application)
    - New General resource classes: **DIGTCRIT, DIGTNMAP**
    - Extensive changes to the RACF **RACDCERT** command
    - New "anchor" user ID: irrmulti
    - Delivered via APARs OW40129, OW40130, rolled back to Release 8

Restricted User IDs

- **Makes use of shared or PUBLIC user IDs safer**
- **Enhancements to ADDUSER, ALTUSER, LISTUSER**
  - ADDUSER xxx RESTRICTED
  - ALTUSER xxx RESTRICTED | NORESTRICTED
- **RESTRICTED: Ignore UACC, ID(*), and GLOBAL when performing access checks**
- **Available on OS/390 V2R8 or V2R9 via APAR OW40129**

OS/390 Release 10

RACF's Certificate Support...

- **OS/390 Release 10**
  - RACDCERT enhancements
    - Support for KeyUsage extension: handshake, dataencrypt, docsign, certsign
    - Support for subjectAltName extension: IP address, Domain name, EMAIL address, URI
    - New certificate export format, PKCS12. Packages certificate chain and user's private key to allow generation of client certificates and standard usage by web browsers.
    - Ability to mark Certifying Authority (CA) certificate as "highly trusted"

RACF's Certificate Support...

- **OS/390 Release 10...**
  - InitACEE enhancements
    - Accepts an optional Host-ID-Mapping extension and assigns the user ID based on that extension
      - ✓ Only from "highly trusted" certifying authorities
      - ✓ Provides a third mechanism for assigning user IDs to a given certificate
  - Certificate Exploiters:
    - IBM HTTP Server
    - CICS client certificate support
    - LDAP Server
    - Host on Demand, eNetwork Host on Demand
    - Firewall Technologies for VPN

RACF's Certificate Support...

- **OS/390 Release 10...**
  - **PKIServe**: A web based Certificate Authority application that utilizes RACF to generate and deliver certificates to end users.
    - Consists of new SAF Callable Service R_PKIServ (IRRSPX00), and sample materials downloaded from from the RACF webpage: http://www.ibm.com/servers/eserver/zseries/zos/racf/webca.htm
  - RACF APAR OW45211, PTF UW74164
  - SAF APAR OW45212, PTF UW74113
  - Roughly Equivalent to the IBM HTTP Server's CaServlet

PKI Sessions

- **Related sessions:**
  - Session 1753, "PKIServ SPE Demonstration", Tuesday, 11:00 AM
  - Session 1743, "z/OS PKI Integration", Thursday, 11:00 AM
  - Session 1744, "Secure z/OS e-Business Solutions", Thursday, 1:30 PM

Selected Other V2R10 Functions

Program Control Usability

- **New diagnostic messages when functions requiring "clean" environment (PADS, execute-control, UNIX server / daemon) fail**
  - Messages will state that failure occurred because of "dirty" environment
  - Messages will give the reason environment became dirty
    - module name, library name, etc.
  - Example: ICH420I PROGRAM PAYROL5 FROM LIBRARY SYS2.PAYLIB CAUSED THE ENVIRONMENT TO BECOME UNCONTROLLED.
- **New RACROUTE REQUEST=AUTH reason code to inform ICHRCX02 that the request would have worked except for dirty environment**
- **Should greatly reduce the need for GTF tracing for Program Control and PADS problems.**

Mixed-Case Profile Name Support

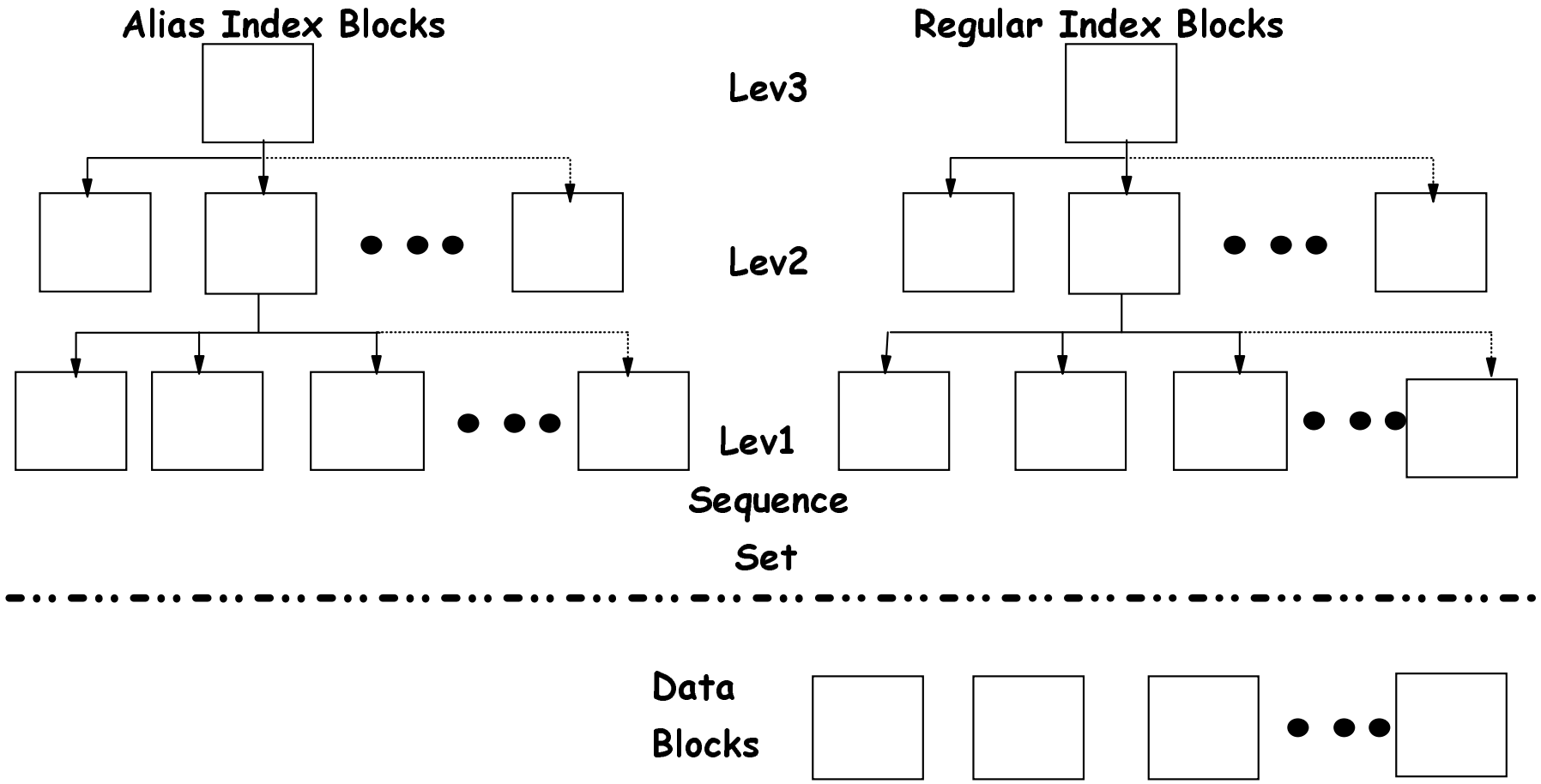
- **Supports Enterprise Java Beans in WebSphere via new classes EJBROLE, GEJBROLE**
- **New CDT option CASE=** UPPER | ASIS allowed for customer-defined classes
- No existing IBM resource classes changed
  - helps ensure compatibility and avoid administrative surprises
- For mixed-case classes, RACF commands and ISPF panels will use profile names as specified by the user
  - RDEFINE EJBROLE (xyz XYZ xYz)
    - defines 3 different profiles
- Also available on OS/390 V2R8 and V2R10 via SPE APAR OW46859
- Full documentation in SYS1.SAMPLIB(IRR46859)

Application Identity Mapping

- **Eliminates need for some kinds of "mapping" profiles:**
  - UNIXMAP -- UNIX UID / GID to user ID or group name
  - NDSLINK -- Novell Directory Services UNAME to user ID
  - NOTELINK -- Lotus Notes (Domino) SNAME to user ID
- **Should:**
  - reduce size of RACF database by eliminating the profiles
  - provide better data integrity in the database
  - provide consistent mapping for shared UIDs or GIDs
  - provide better performance than UNIXMAP profiles
- **Uses new "alias" index structure in RACF data base**

Alias Index Structure...

- Alias IX blocks, are similar to regular IX blocks at upper levels. In the Sequence Set, instead of pointers to data profiles, Alias IX entries contain base profile info.



RACF Support for DB2 V7

- **Overview: New DB2 Version 7 Function**
  - The JAR object and USAGEAUTJ privilege
  - Database names(s) bass on DBADM privilege check for CREATE VIEW, ALTER INDEX, and DROP INDEX if DB2 DBADM CREATE AUTH is set on
    - Multiple data bases may be passed on a CREATE VIEW request
  - Database name also passed on a CREATE ALIAS request

RACF Support for DB2 V7...

- **DB2 DSNX@XAC supports a reason code of x'10' (16) on initialization. This new reason code instructs the DB2 subsystem to terminate if:**
  - An abend occurs in the DSNX@XAC exit
  - The DSNX@XAC exit instructs DB2 to no longer call it
  - An unexpected return code is returned to DB2 from the DSNX@XAC exit
- **Generally available March 2001**

RACF Support for DB2 V7...

- **Changes to ('SYS1.SAMPLIB(IRR@XACS)'):**
  - Code to process the specification of a database name on a ALTER INDEX and DROP INDEX request if the XAPLCRVW is on
  - Code to process the specification of a set of database names on a CREATE VIEW request if the XAPLCRVW bit is on
  - A new exit option (&ERROROPT) is introduced to support the new DB2 reason code
  - Two new classes: MDSNJR/GDSNJR
  - Delivered with APAR OW45152

RACF Support for DB2 V7...

- **&ERROROPT instructs DB2 what to do when an unexpected error occurs in the DSNX@XAC exit. An unexpected error is:**
  - An abend occurs in DSNX@XAC
  - An unexpected return code is returned by DSNX@XAC
  - DSNX@XAC instructs DB2 to not call it again

RACF Support for DB2 V7...

- **&ERROROPT=1**
  - Defer to DB2 when an "unexpected error" (see above) occurs
  - Default
- **&ERROROPT=2**
  - The DB2 subsystem is instructed to terminate if an "unexpected error" occurs
  - Only effective for DB2 Version 7

RACF Support for DB2 V7...

- **DB2 V7 Introduces a new message:**
  - **DSNX210I** *csect-name* **- ACCESS CONTROL AUTHORIZATION EXIT (DSNX@XAC) AS INDICATED THAT IT SHOULD NOT BE CALLED, HAS ABENDED, OR HAS RETURNED AN INVALID RETURN CODE DURING** *function-code***. RETURN CODE=***return-code***, REASON CODE=***reason-code*
- *New corresponding SQL return code of X'00E70015'*

RACF/DB2 Session

- See session 1734, "RACF and DB2:Teamed for Security" Wednesday, 1:30 PM for details.

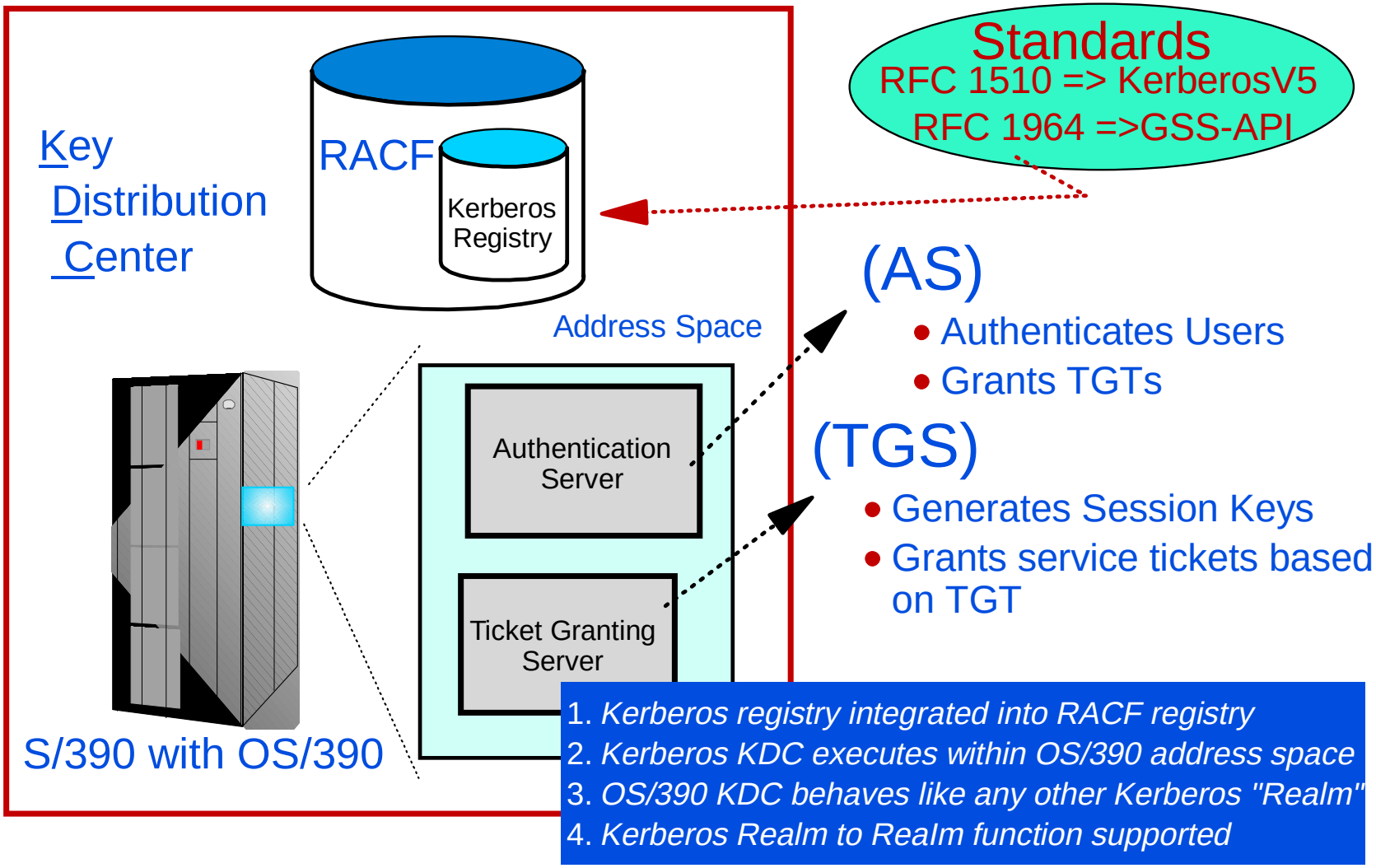
Network Authentication Service

- **New Security Server component**
  - licensed with OS/390 base, for all OS/390 customers, like the LDAP server
  - requires RACF support or compatible other security product
- **OS/390 implementation of MIT's Kerberos Version 5**
- **Provides services for:**
  - USER AUTHENTICATION
  - DELEGATION
  - DATA CONFIDENTIALITY
- **Interoperates with other industry Kerberos Version 5 implementations**
- **Can provide consistent user authentication for Kerberos-aware applications spanning a network including, e.g. OS/390, Windows 2000, UNIX, AS/400**

Network Authentication Service...

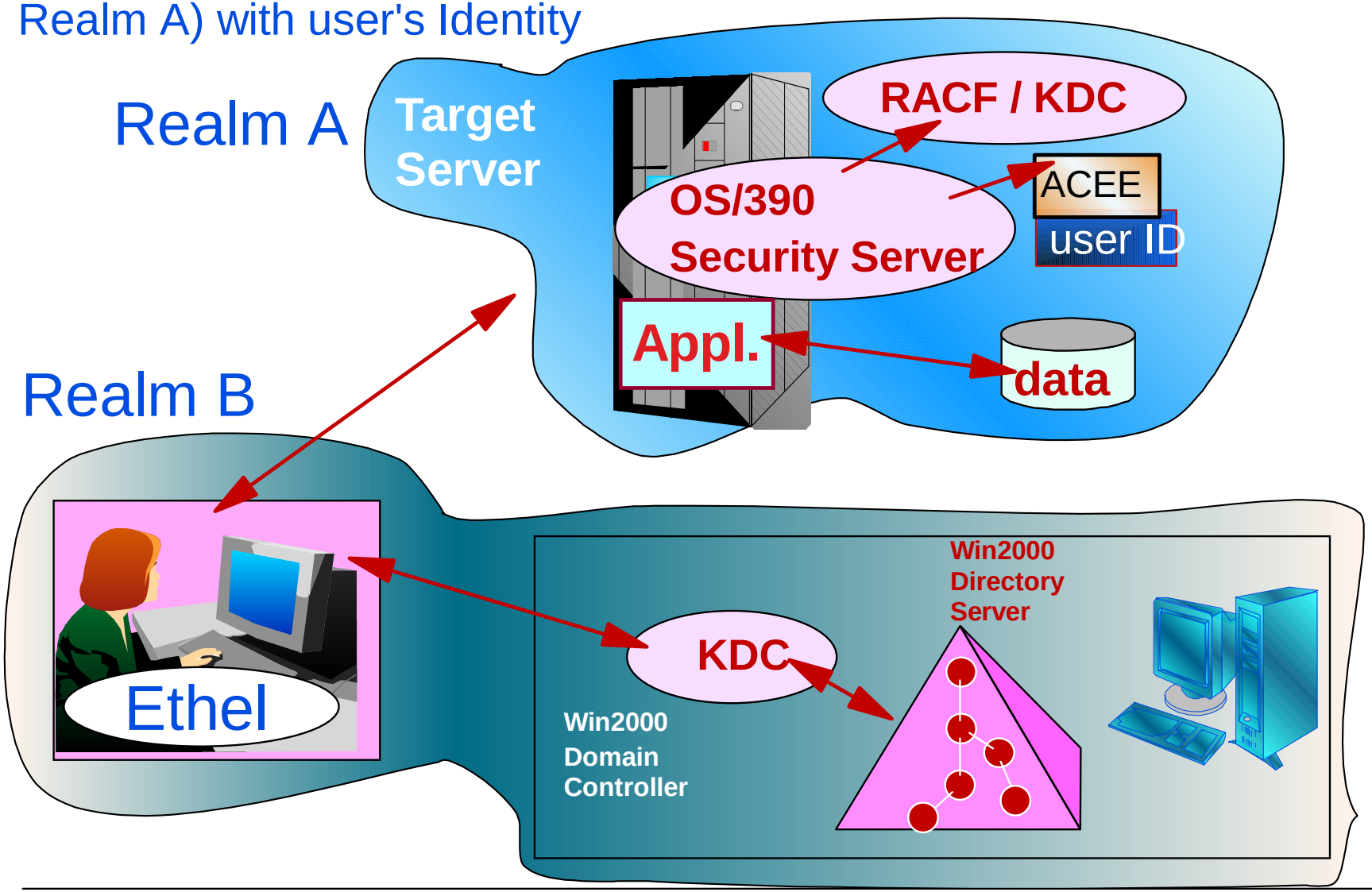
- **RACF provides support for the server:**
  - definition of local Kerberos principals (users)
    - KERB segment
  - definition of the local Kerberos realm& foreign realms
    - REALM class
  - definition of foreign Kerberos principals with a local identity
    - KERBLINK profiles
  - Basically, the RACF database ***IS*** the Kerberos registry for OS/390
  - RACF password ***IS*** the user's Kerberos password
- **Server uses SAF callable services to interact with RACF: parse Kerberos tickets to obtain principal names; map from principal to RACF user and vice versa**
  - Enhanced R_usermap service
  - new R_kerbinfo service
  - new R_ticketserv service

Network Authentication Service...



Network Authentication Service Example

Scenario: User defined to Win2000 Active Directory (Kerberos Realm B) wishes to access application on OS/390 (Kerberos Realm A) with user's Identity



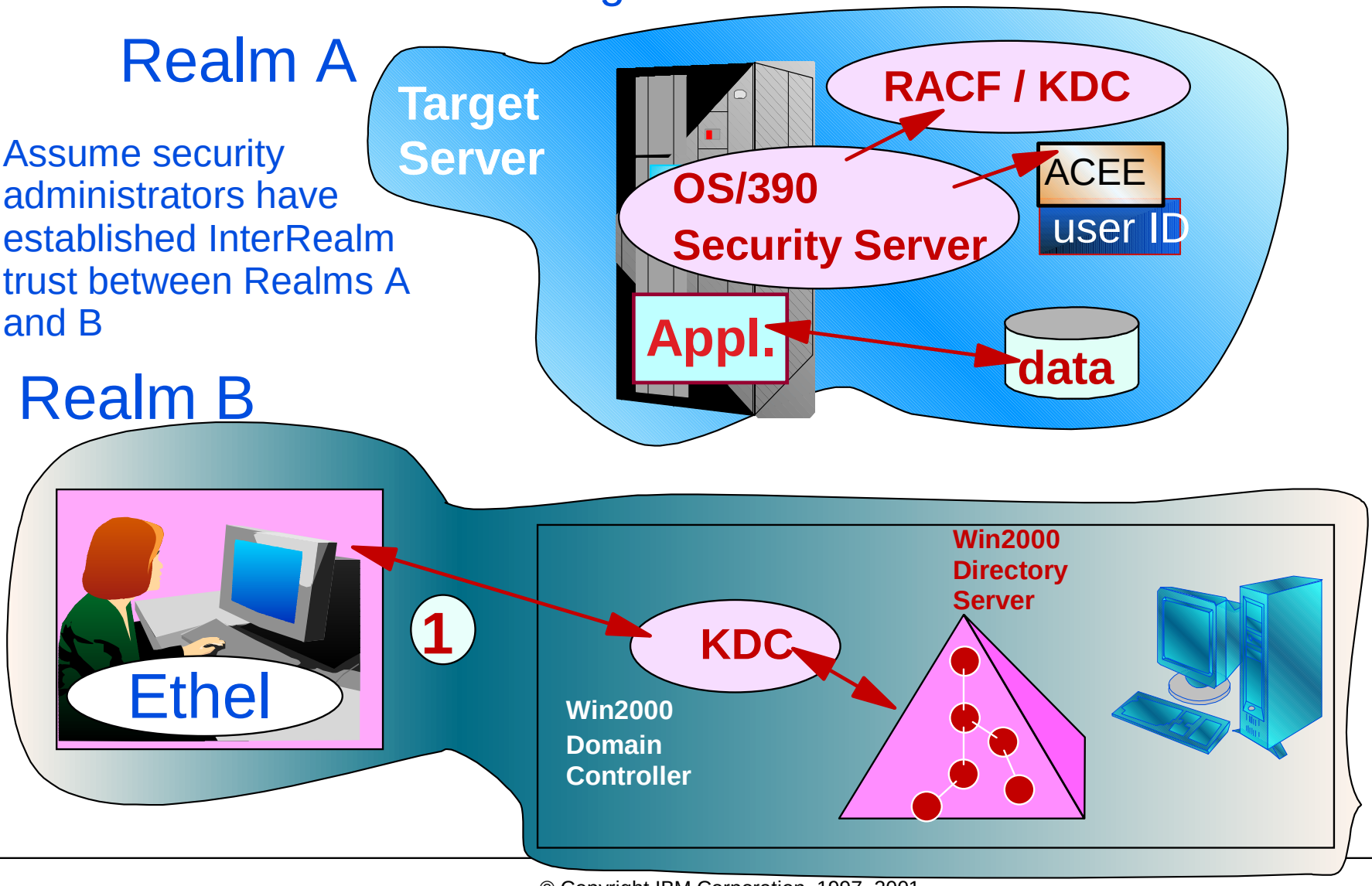
Network Authentication Service Example...

1- The client authenticates to the Win2000 KDC, and obtains a ticket for the target server.

Realm A

Assume security administrators have established InterRealm trust between Realms A and B

Realm B



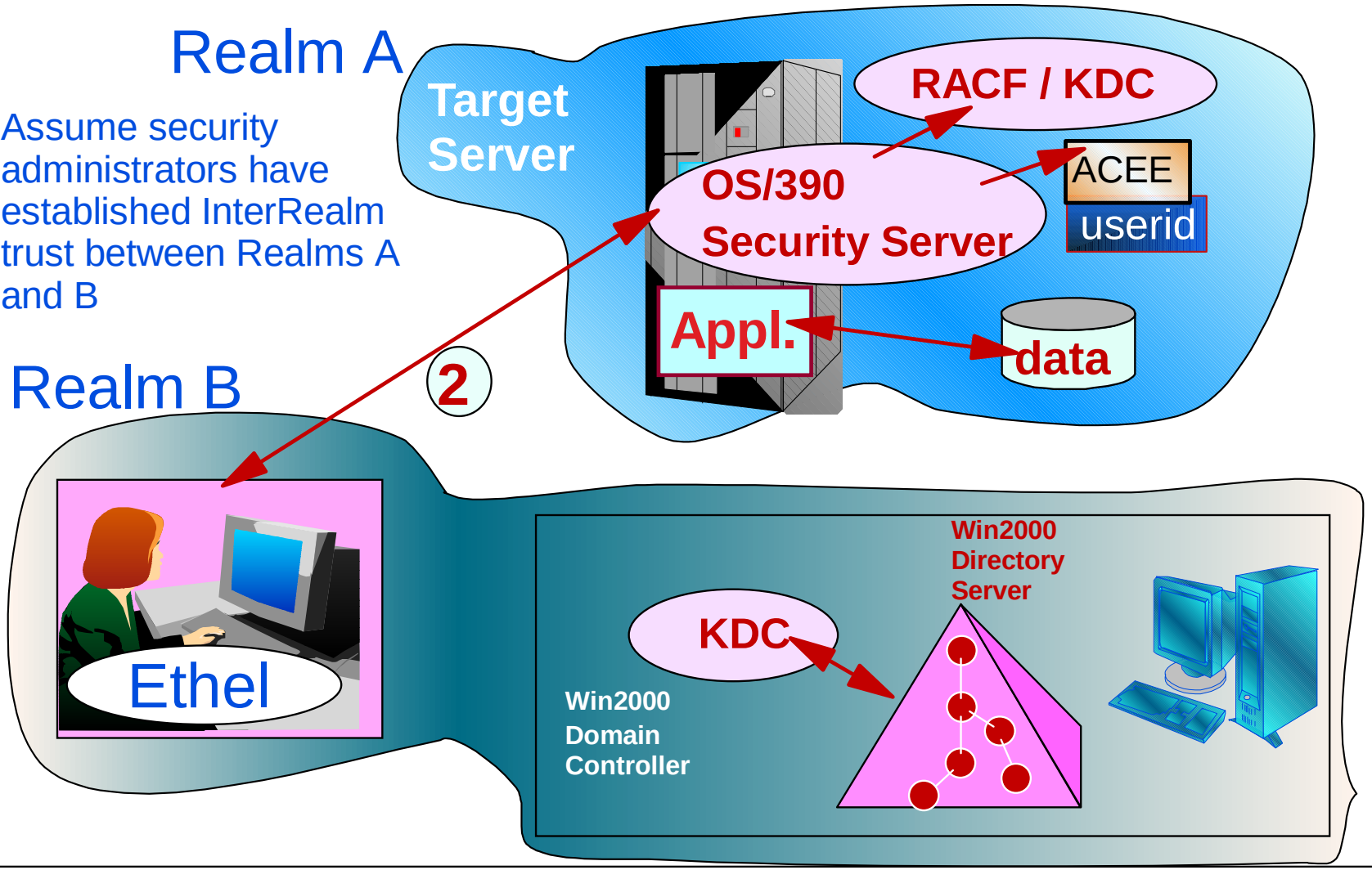
Network Authentication Service Example...

2- On OS/390, target application using SAF services, validates the ticket, and if necessary, via SAF / RACF maps the Kerberos principal contained in the ticket to an OS/390 User ID.

Realm A

Assume security administrators have established InterRealm trust between Realms A and B

Realm B



Kerberos on S/390 Sessions

- **Related sessions:**
  - Session 1726, "Kerberos on z/OS Part I:Overview", Tuesday, 4:30 PM
  - Session 1727, "Kerberos on z/OS Part II: Implementation", Tuesday, 6:00 PM

LDAP Server Enhancements

- **Enhancements for customer (not RACF) data in LDAP**
- **LDAP V3 Schema Publication and Update**
  - Better interoperation with other LDAP V3 servers on other platforms
  - Allows administrators to dynamically add and modify LDAP schema describing their information
  - Eliminates server restart after changing schema
  - Allows LDAP clients to query the schema definition using LDAP
- **Bulk load utility**
  - Allows loading of large numbers of directory entries into the server
  - Eases migration of data from other platforms to OS/390
  - Eases migration of data from test into production
- **Greatly increased storage capacity**
  - Single server can manage millions of directory entries across multiple DB2 databases

LDAP on S/390 Sessions

- **Related sessions:**
  - Session 1724, "OS/390 Security Server: LDAP Overview and Announcements" , Tuesday 1:30 PM
  - Session 1727, "OS/390 Security Server: LDAP Usage and Demonstration", Tuesday, 3:00 PM

Network Security and Usability

- **Functions provided by SecureWay Communications Server for OS/390**
- **TN3270E Server SSL enhancements**
  - Implements SSL negotiation based on enterprise security policy
  - Can force use of SSL based on IP address, hostname, or link
  - Allows use of same port for SSL and non-SSL, simplifying server and client configuration
- **TCP/IP protection of network resources**
  - Controls OS/390 users' access to
    - TCP/IP stack
    - TCP or UDP port
    - Network
  - Uses profiles in the SERVAUTH class
  - Allows grouping of network IP addresses into a "security zone" that you can protect as a RACF resource.

Network Security and Usability ...

- **Virtual Private Network "On-Demand" Tunnels**
  - Tunnel: An encrypted data pipe from one system to another
  - Before OS/390 V2R8: configured manually by the administrator
  - With OS/390 V2R8: dynamic configuration (key exchange) possible
    - clients could request creation of tunnel for data sent to OS/390
    - or administrator could manually create one for data sent from OS/390
  - New support: Policy can cause automatic creation of tunnels for data sent from OS/390, too.

Comm Server Session

- See session 1741, "Communications Server for z/OS TCP/IP Network Security Features", Thursday 8:00 AM for details.

z/OS R2 RACF Enhancements

UNIVERSAL Groups

- **Goal: You want to connect many (say, 10K) users to a group**
- **Problem: RACF limits you to 5957 users per group**
- **z/OS R2 solution: ADDGROUP xyz UNIVERSAL**
  - Can have an unlimited number of regular users (USE authority)
  - Limit of 5957 still applies to users with more privilege:
    - users with CREATE, CONNECT, or JOIN in the group
    - users with group-SPECIAL, group-OPERATIONS, or group-AUDITOR
  - Available only for ADDGROUP, not ALTGROUP

UNIVERSAL Groups...

- **CONNECT user1 GROUP(xyz) AUTH(use)**
  - updates user1 USER profile to show a connection to xyz.
  - does not update xyz GROUP profile.
- **LISTGRP xyz will not show the regular users**
  - they are not actually present in the GROUP profile
  - listing would be difficult to use given its size, anyway
  - for reporting, use IRRDBU00 output
- **LISTUSER user1 will show xyz as one of the user's groups**
- **RACROUTE REQUEST=VERIFY will include xyz in the ACEE**
  - access lists with xyz in them will work as you expect

SAF Trace

- **Provides tracing of RACROUTE, SAF callable service, and ICHEINTY requests to aid problem diagnosis**
- **Enabled via RACF subsystem SET TRACE command**
- **Can specify which requests to trace and which address spaces to trace**
  - Example: SET TRACE(JOBNAME(xyz) RACROUTE(TYPE(1)))
    - will trace all RACROUTE REQUEST=AUTH from job xyz
  - SET TRACE(ASID(25) DATABASE(ALTER))
    - will trace all ICHEINTY ALTER, ADD, DELETE, RENAME from address space 25
- **Trace goes to GTF, like other RACF SET TRACE output**
- **Use IPCS to read the trace, with the GTF USR command**

Cross-System VLF Enhancement

- **IRRACEE class in VLF helps improve performance by caching ACEEs for later reuse**
- **Problem: If system A and system B share the RACF database, a USER profile change from system A will purge all the cached ACEEs on system B**
- **Solution: Use XCF to communicate between z/OS R2 systems:**
  - System A can tell system B exactly which ACEE changed
  - System B can purge just the changed ACEEs, not all of them
  - Requires RACF sysplex communications
- **Does not help in all cases:**
  - Group changes or port-of-entry changes could still cause purging
  - However: most purging comes from user profile changes

Coupling Facility Error Enhancement

- **RACF Data Sharing mode uses Coupling Facility (CF) in a sysplex as a large data buffer**
- **Improves performance**
- **Problem: CF errors treated as RACF database I/O errors**
  - Can cause ABENDs
  - Has caused problems like IMS subsystem failures
- **Solution: In z/OS R2, if CF failure occurs, RACF will attempt to wait for a CF REBUILD operation to fix the problem, and retry the CF operation**

Other z/OS R2 Security Server Enhancements

z/OS R2 Network Authentication Service Enhancements

- **Supports three Kerberos encryption methods:**
  - DES (previously supported in R10)
  - Triple DES
  - DES with derivation keys
- **Supplies kpasswd and kadmin client commands to run on z/OS**
  - allows administration of foreign Kerberos realms.
- **Additional exploiters:**
  - LDAP server and client
  - FTP, TELNET, RSH

z/OS R2 LDAP Server Enhancements

- **Ability to manage USER->GROUP connections**
  - i.e. CONNECT command support
- **Support for LNOTES, NDS, and KERB segments for USER profiles**
- **Ability to search for a**
  - USER via UID
  - GROUP via GID
- **Support for authentication via Kerberos V5**

z/OS R2 SSL & Digital Certificate Enhancements

- **System SSL will check for revoked certificates when issued by PKIX compliant certificate authorities.**
  - increases server security when using digital certificates for client authentication
- **System SSL supports new TLS (Transport Layer Security) IETF standard**
- **Communications Server SSL and TLS support for FTP**
- **Communications Server Kerberos support for FTP, TELNET, and RSH**
- **Communications Server handling of certificates via Express Logon improved (2-tier solution)**

Reminder!

Service End Dates

Reminder: Service End Dates

- **Already out of service:**
  - RACF V2 and MVS/ESA V5
  - OS/390 V1 (including Security Server components)
  - OS/390 V2R4 (including Security Server components)
  - OS/390 V2R5 (including Security Server components)
- **March 31, 2002:**
  - OS/390 V2R6

References

- RACF Command Language Reference (SC28-1919)
- RACF Macros and Interfaces (SC28-1914)
- RACF Security Administrator's Guide (SC28-1915)
- RACF Auditor's Guide (SC28-1916)
- RACF Callable Services Guide (SC28-1921)
- OS/390 Security Server Open Cryptographic Enhanced Plug-ins (OCEP) Guide and Reference (SA22-7429)
- OS/390 OCEP Module Developer's Guide and Reference (SC24-5876)
- OS/390 OCEP Application Developer's Guide and Reference (SC24-5875)
- OS/390 Security Server LDAP Server Administration and Usage Guide (SC24-5861)
- OS/390 Security Server LDAP Client Application Development Guide and Reference (SC24-5878)

References...

- **Or on the web, in either PDF or Book Manager formats:**
  - Security Server for OS/390 V2R10:
    - Book Manager:
      http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICH1K131
    - PDF:
      http://www-1.ibm.com/servers/s390/os390/bkserv/r10pdf/secserv.html
  - OS/390 library: http://www.ibm.com/servers/s390/os390/bkserv/
  - z/OS library : http://www.ibm.com/servers/eserver/zseries/zos/bkserv/
  - General Site:
    http://publibfp.boulder.ibm.com:80/cgi-bin/bookmgr/LIBRARY

RACF Home Page

- **http://www.ibm.com/servers/eserver/zseries/zos/racf**
  - Latest release information on RACF
  - Links to announcement letters
  - Sample code
    - DBSYNC to compare/sync. two RACF data bases
    - RACFICE to create audit/analysis reports
    - OS390ART for a web-based reporting tool
    - RACTRACE tracing facility
    - RACFDB2 Conversion Utility
  - Frequently Asked Questions
  - RACF user group information
  - RACF-L information
  - Presentations on RACF-related topics

OS/390 Security Home Page

- **http://www.ibm.com/servers/eserver/zseries/zos/security**
  - Overview of security concepts, including animations
  - Overview of S/390, zSeries, OS/390, and z/OS security functions
  - Links to related web sites for OS/390 and z/OS components

OS/390 and z/OS Security Server

RACF Update

Mark Nelson
RACF Development
IBM Corporation
2455 South Road
Poughkeepsie, NY 12601l
(845) 435-7758
markan@us.ibm.com

SHARE
Session 1732
July 2001