LDAP Implementation and Customization on 390 (SHARE Session 2945)

Tim Hahn
IBM OS/390 LDAP Development
hahnt@us.ibm.com

Technology • Connections • Results

What is a Directory?

- Listing of information about objects - phone directory, library card catalog
- Specialized database - read bias, static data, not transaction based (atomic)
- Not a general purpose database but a limited function database
- Usually distributed (client/server) with a defined API interface (LDAP)
- Security based on authentication (network security) and ACLs (access control lists)

Why is a Directory Service Important?

- ➤ Example - Domain Name Service (DNS). We use it everyday - without it we wouldn't find services on the Internet.
- ➤ Within an Intranet or across the Internet there is a need to provide "locating information". Example - BigYellow.com.
- ➤ In addition, remote, distributed, single point of control is necessary for Enterprise Management. Example - DEN (Directory Enabled Network).
- ➤ Some view this as the key to PKI (Public Key Infrastructure) and Single Sign-On.

What is LDAP?

- LDAP - Lightweight Directory Access Protocol
- de-facto Internet (TCP/IP-based) wire protocol for accessing and updating directory information
- "V2" defined in Internet Drafts
- "V3" defined in IETF RFCs 2251-2256, 2829, 2830
- New RFCs all the time (e.g. RFC 2849 - LDIF format)

The IBM LDAP Solution

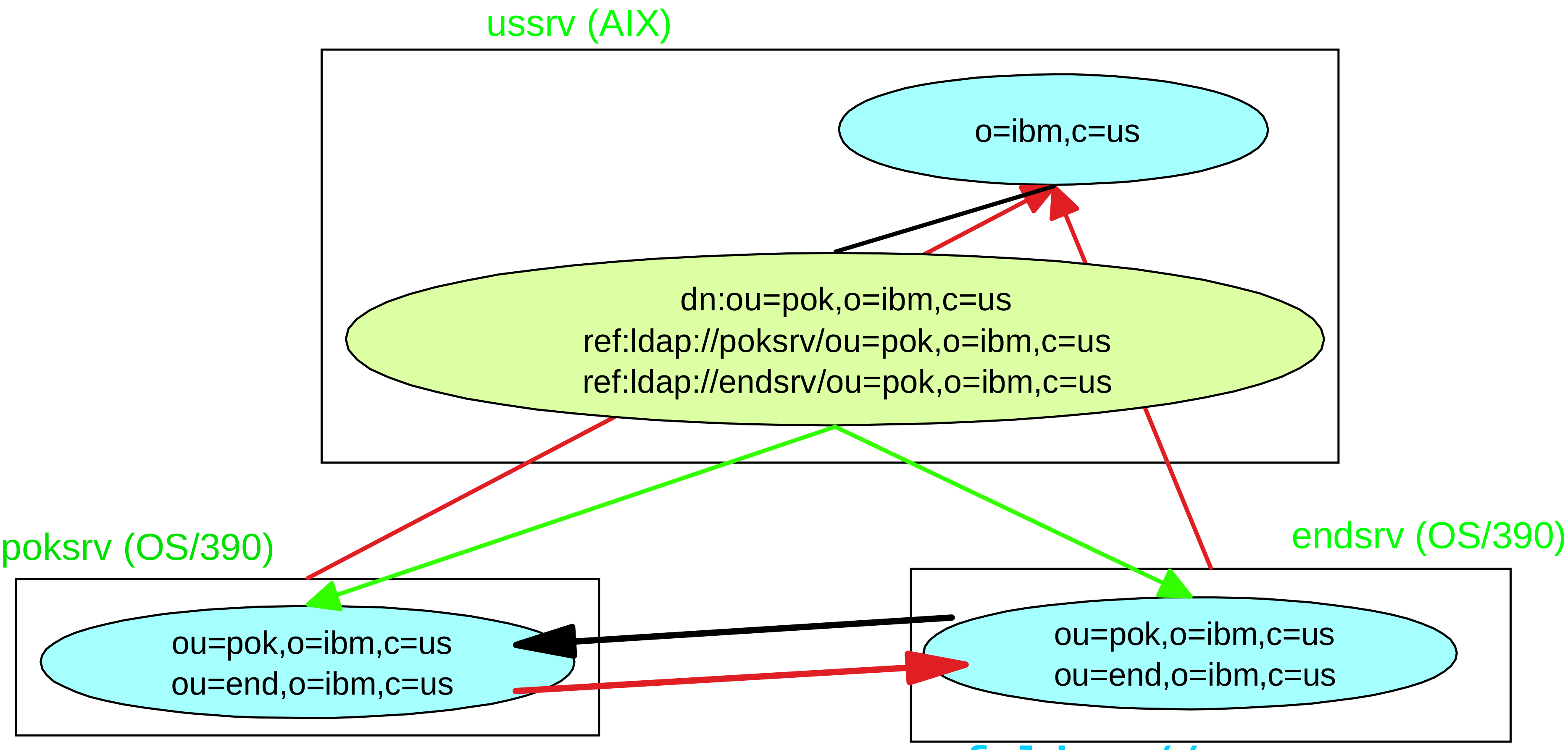
- SecureWay Directory - part of SecureWay brand due to strong ties with Security offerings
- AIX, OS/390, AS/400 products:
  - LDAP V3 protocol
  - DB2 backing store
- Each platform has made enhancements

IBM Interoperability

- ➤ No standards (yet!) for replication or Access control, although there are recent Internet drafts
- ➤ IBM offerings implement these in the same way
- ➤ Namespace can be split among servers using referrals
- ➤ Replication between platforms is available, within bounds
- ➤ Access control lists understood cross-platform, within bounds

Namespace Example Using Referrals and Replication

:xample using referrals and replication



```
ref ldap://ussrv
```

```
ref ldap://ussrv
masterserver ldap://poksrv
masterserverDN "cn=master"
```

Technology • Connections • Results

LDAP on OS/390

- ➤ Server packaged as part of the OS/390 Security Server
- ➤ Client packaged as part of the OS/390 base prior to OS/390 2.8
- ➤ With OS/390 2.8, both server and client packaged as part of the OS/390 Security Server, always enabled
- ➤ Many possibilities for OS/390 server configuration:
  - ➤ sysplex, multiserver, or single server
  - ➤ DB2, RACF, or both
  - ➤ Secure socket, normal socket, or both

LDAP on OS/390

- ➤ Makes use of Unix System Services file system
- ➤ Configuration files install into /usr/lpp/ldap/etc
  - ➤ Can be moved to datasets
- ➤ Default location for configuration and environment files is /etc/ldap
  - ➤ Customized configuration files can be moved here or full path name can be specified to LDAP Server at start-up (or specify by DD card for started task)
- ➤ Client API documentation files (html) installed into /usr/lpp/ldap/doc

- ➤ z/OS R1 - use new LDAP Configuration Utility - LDAPCNF

Starting the LDAP Server

- DB2 V5,V6, or V7 is required in order to use the DB2 backing store of the LDAP server
- A sample configuration is provided but must be localized to the system/installation
- A sample configuration setup is also provided in /usr/lpp/ldap/examples/sample_server
- STEPLIB must be setup prior to running the LDAP server (or add PDS(s) to LNKLST)
- PDS holding DLLs is <GLDHLQ>.SGLDLNK
- z/OS R1 - use new LDAP Configuration Utility - LDAPCNF

Starting the LDAP Server - 2

- Set up DB2 and start DB2
  - Enable CLI
  - <DB2HLQ>.SDSNLOAD in STEPLIB or LNKLST
- Bind Plan for CLI (DSNTIJCL sample)
- Run LDAPTBL.JCL to create database, tablespaces, and tables
- Modify the slapd.conf file for the system
- Using RDBM
  - Run ldif2db (or GLDLD2DB JCL) to prime the Directory
- Using TDBM
  - Run ldf2tdbm (or LDF2TDBM JCL) to prime the Directory
- Run slapd (or LDAPSRV JCL) to start the Directory Service
  - (Sample JCL can be found in <GLDHLQ>.SGLDSAMP PDS).

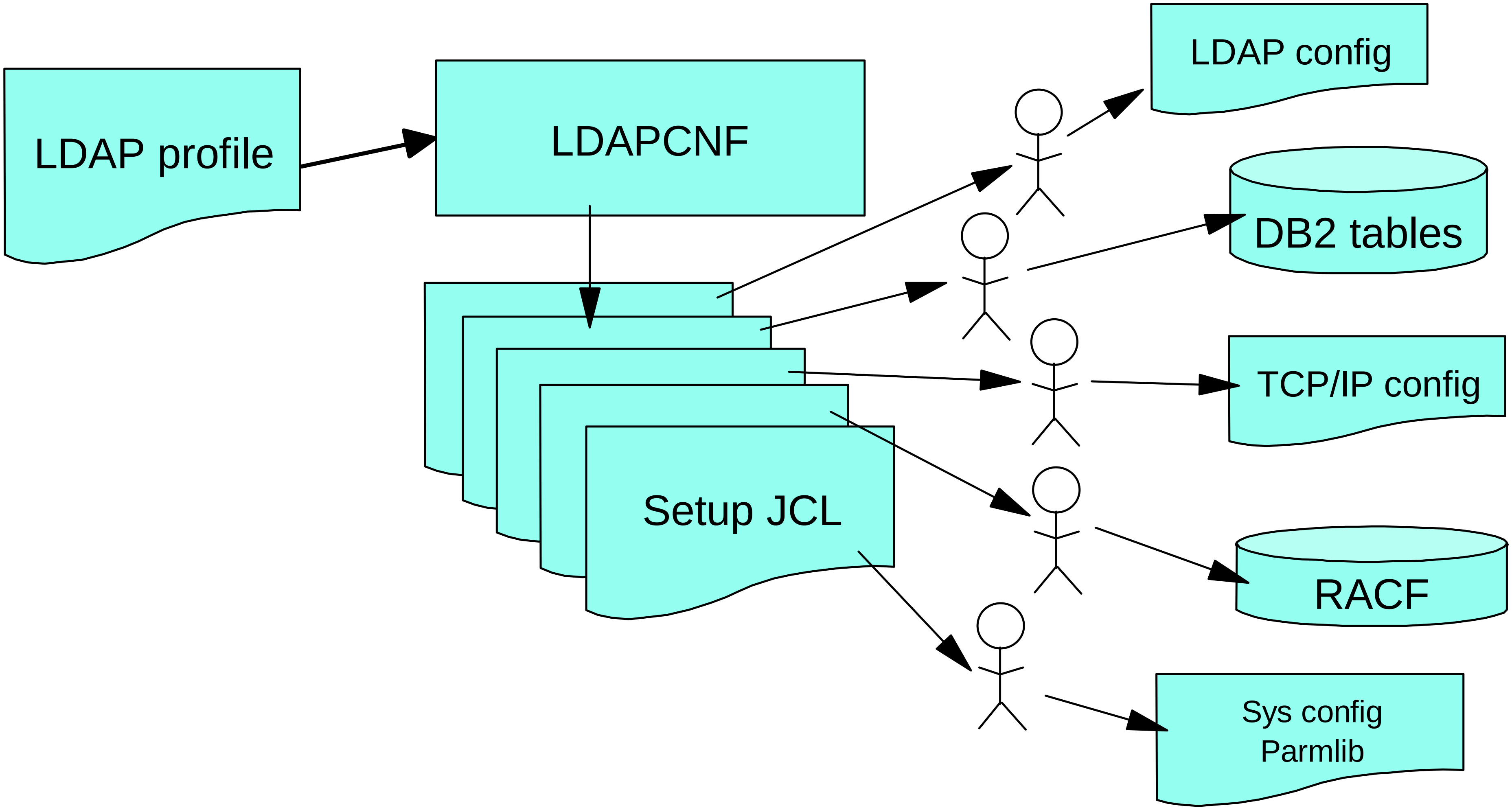
Starting the LDAP Server - 3

- ► DB2 is not required if only accessing RACF data through LDAP
- ► STEPLIB must still be set for locating LDAP DLLs prior to running the server (or add PDS to LNKLST)
- ► LDAP PDS (<GLDHLQ>.SGLDLNK) plus other datasets must be APF-authorized and protected (or program-controlled)
- ► If configuring for both DB2 and RACF backing stores, the dataset containing the DB2 CLI DLL must also be APF-authorized and protected (or program-controlled)
- ► Modify the slapd.conf file for the system

LDAP Configuration Utility

- Streamlines implementation of LDAP servers on a system
- Input is a set of parameter files
- Output is a set of batch jobs (JCL)
- Batch jobs should be verified by
  - Network Administrators
  - Database Administrators
  - Security Administrators
  - System Programmers
  - LDAP Administrators
- Once acceptable, batch jobs should be submitted which will create the necessary configurations and settings for the server

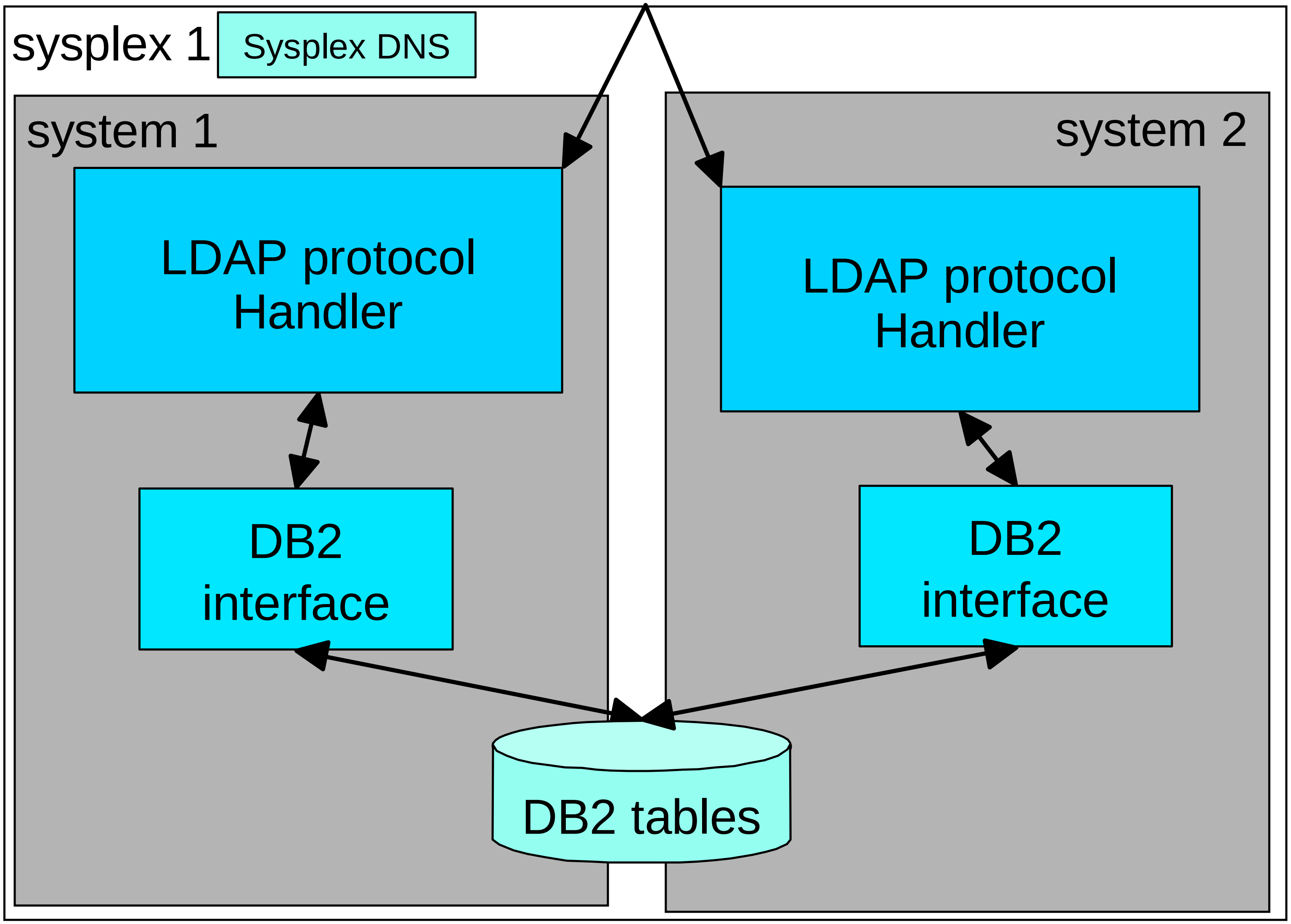
LDAP Configuration Utility



Sysplex Support

- Multiple LDAP Servers can operate on the same DB2 tables which are made available across a sysplex using DB2 data sharing
- Exploits Sysplex DNS and TCP/IP connection optimization for load balancing across the sysplex
- Requires sysplex to be running in GOAL mode

Sysplex Support



How to setup Sysplex support

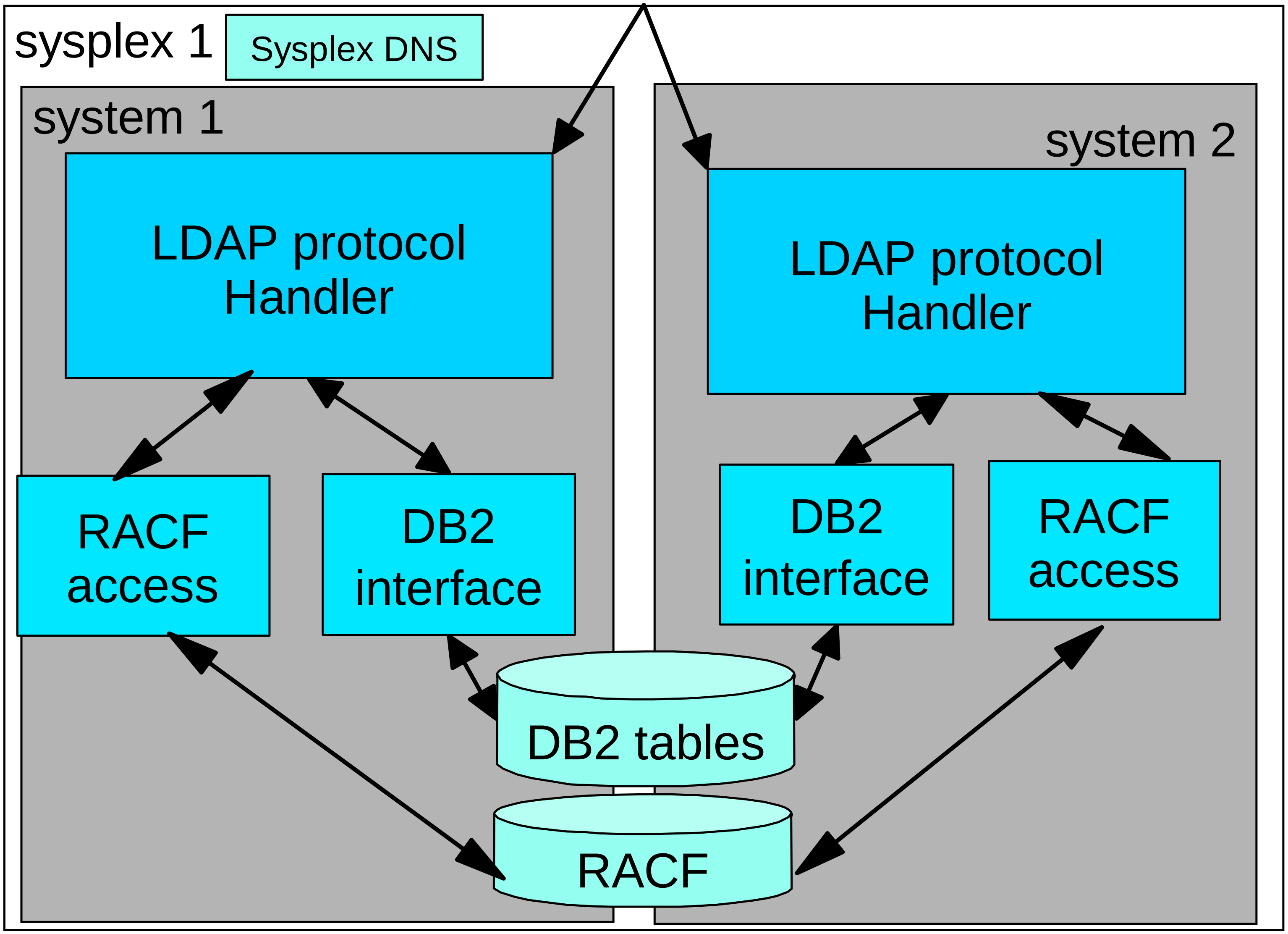
- Configuration file keywords:
  - **SYSPLEXGROUPNAME** - name of the WLM group for the set of LDAP Servers
    SYSPLEXGROUPNAME   ldapgrp1
  - **SYSPLEXSERVERNAME** - name of the particular server within the group
    SYSPLEXSERVERNAME   srv1
- LDAP clients using the SYSPLEX DNS name will be routed to LDAP servers running on multiple machines in the sysplex
  - Example: for set of LDAP servers on sysplex1, defined as ldapgrp1, all listening on port 389:

```
ldapsearch -h ldapgrp1.sysplex1 -p 389 ...
```

Security Server Access Support

- Implemented as a new "back-end" to the LDAP server
- USER and GROUP RACF profiles appear as a subtree of entries in the LDAP namespace
- Bind, add, modify, delete, and search LDAP protocol operations are supported
- Access controls for USER and GROUP profiles enforced by Security Server
- APAR OW41515 enhances bind support: password change as well as more information for a failed bind attempt

Security Server Access Support



How to Setup Security Server Support

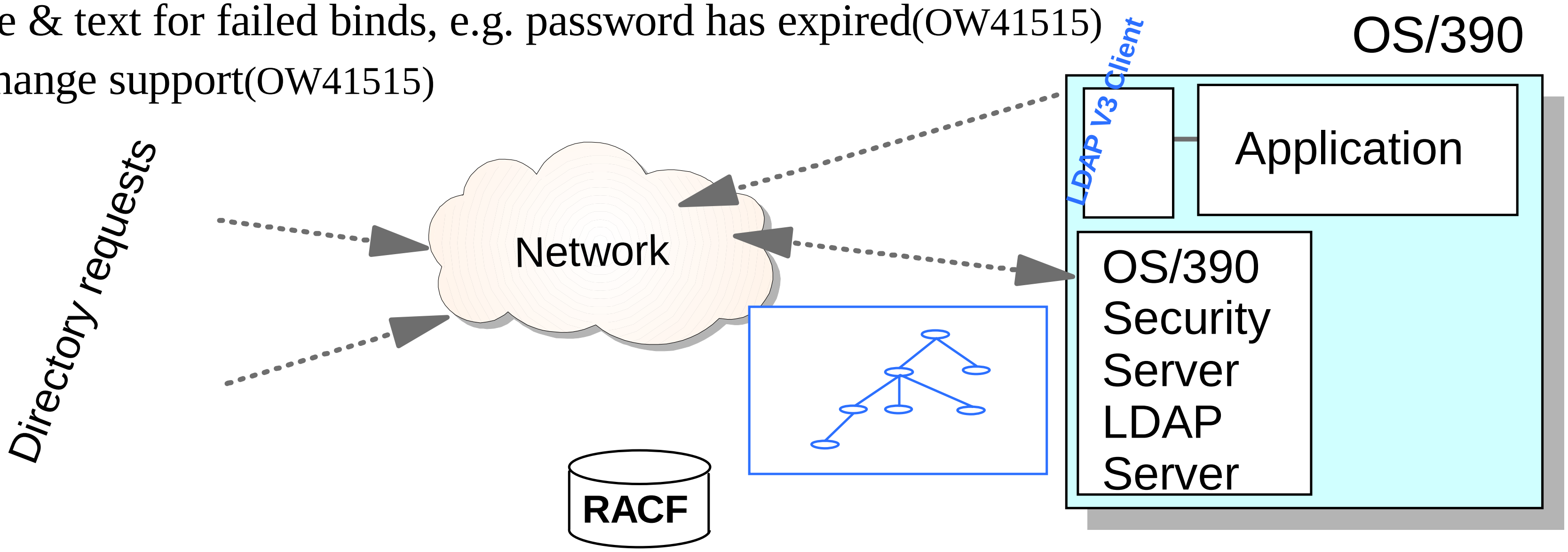
- Add configuration keywords to LDAP Server configuration file:

```
database sdbm GLDBSDBM
suffix "cn=plex1, o=IBM, c=US"
```

- Requires APF authorization and Program Control
- Re-start the LDAP server

RACF Functions that LDAP Server Supports

- User and Group Commands and Information
- Add or Delete Users and/or Groups
  - ➤ ADDUSER (AU) and DELUSER (DU) Commands
  - ➤ ADDGROUP (AG) and DELGROUP (DG) Commands
- Modify and Retrieve Information on Users and/or Groups
  - ➤ LISTUSER (LU) and ALTUSER (ALU) Commands
  - ➤ LISTGRP (LG) and ALTGROUP (ALG) Commands
- Supports LDAP Binds (Using RACF Password Verification)
  - ➤ Reason code & text for failed binds, e.g. password has expired(OW41515)
  - ➤ Password change support(OW41515)

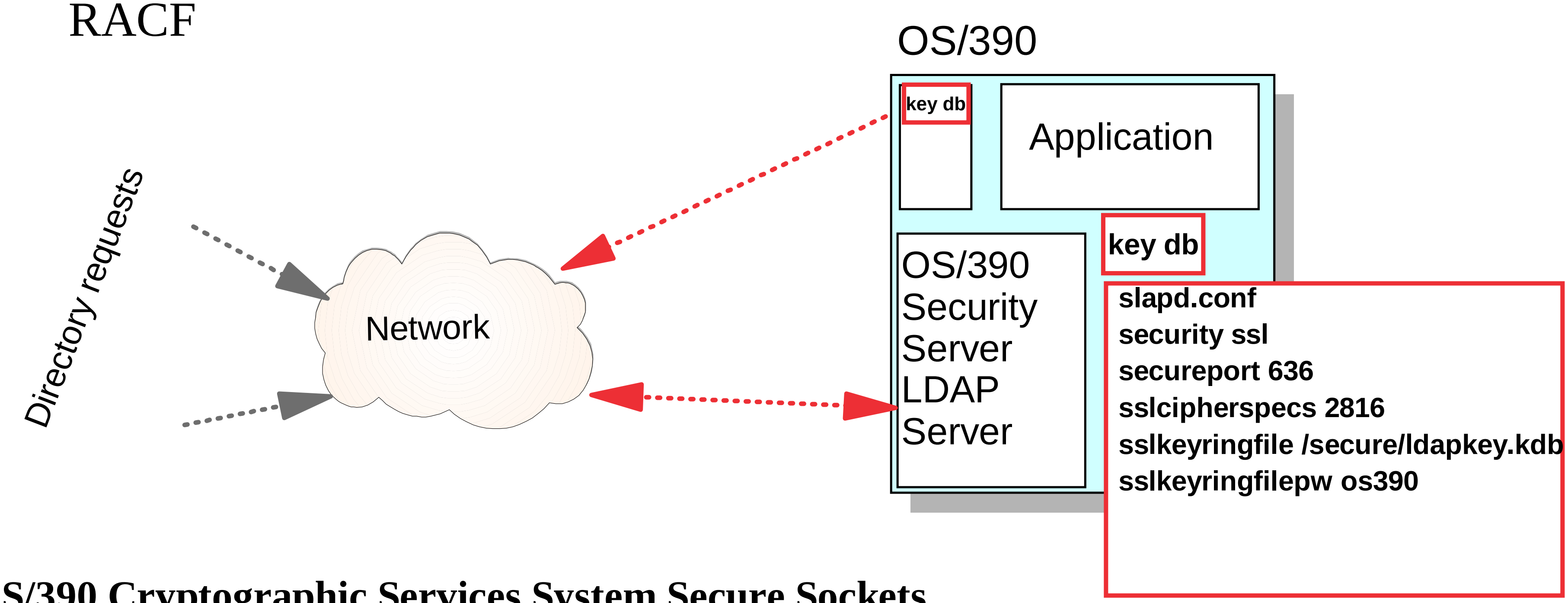


LDAP Server And SSL

- LDAP Server can be set up to listen on a combination of secure and non-secure ports
- Default non-secure port is 389
- Default secure port is 636
- LDAP Server and Client use System SSL, also part of the OS/390 Security Server, for SSL connections and key-database management

LDAP Server Requirement for SSL Support

- Uses System SSL (OS/390 2.7)
- Uses Server Authentication (prior to OS/390 2.8)
- Uses Client and Server Authentication (OS/390 2.8)
  - With APAR OW41326 LDAP server can use certificates in RACF

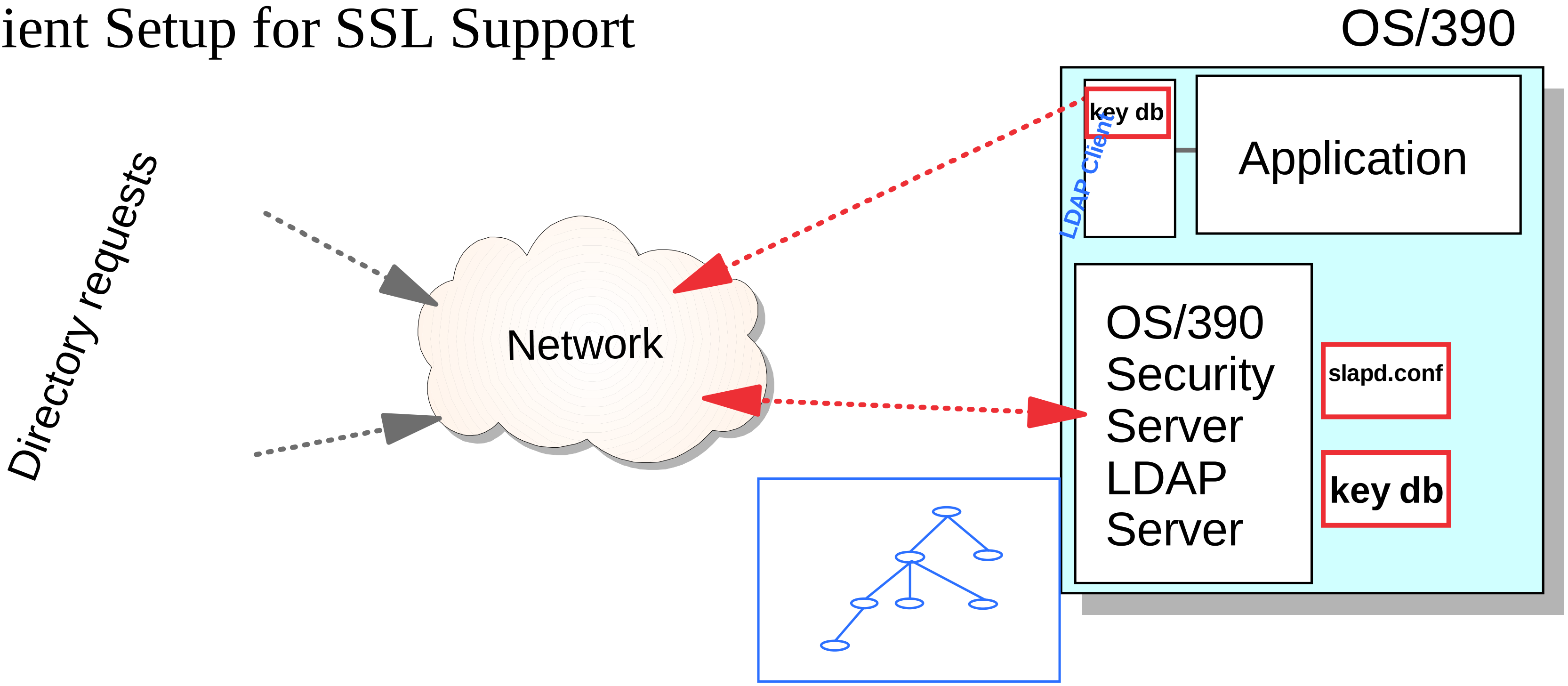


```
slapd.conf
security ssl
secureport 636
sslcipherspecs 2816
sslkeyringfile /secure/ldapkey.kdb
sslkeyringfilepw os390
```

OS/390 Cryptographic Services System Secure Sockets Layer Programming Guide - SC24-5877

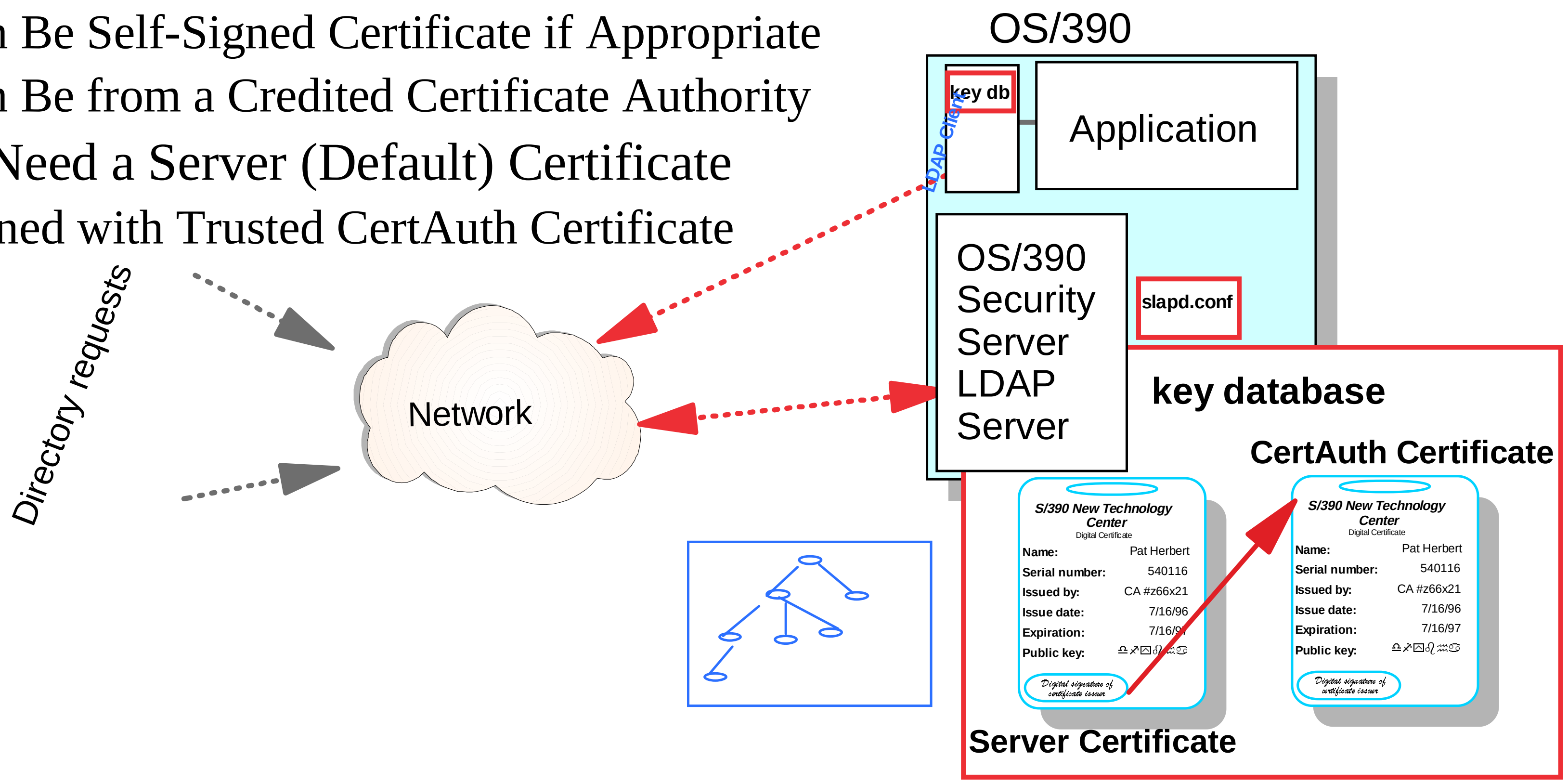
Securing the OS/390 LDAP Server with SSL

- ➤ LDAP Server Setup for SSL Support
  - ➤ Server Customization
    - ➤ Configuration Files
  - ➤ LDAP Server Setup for Key Management
- ➤ LDAP Client Setup for SSL Support



LDAP Server Setup for Key Mgmt

- Build a Key Database and Fill with Certificates
  - ➤ Can use RACF to keep the certificates
  - ➤ Or use **`gskkyman`** for Key Management
  - ➤ Need a Trusted CertAuth Certificate
    - ➤ Can Be Self-Signed Certificate if Appropriate
    - ➤ Can Be from a Credited Certificate Authority
  - ➤ Also Need a Server (Default) Certificate
    - ➤ Signed with Trusted CertAuth Certificate

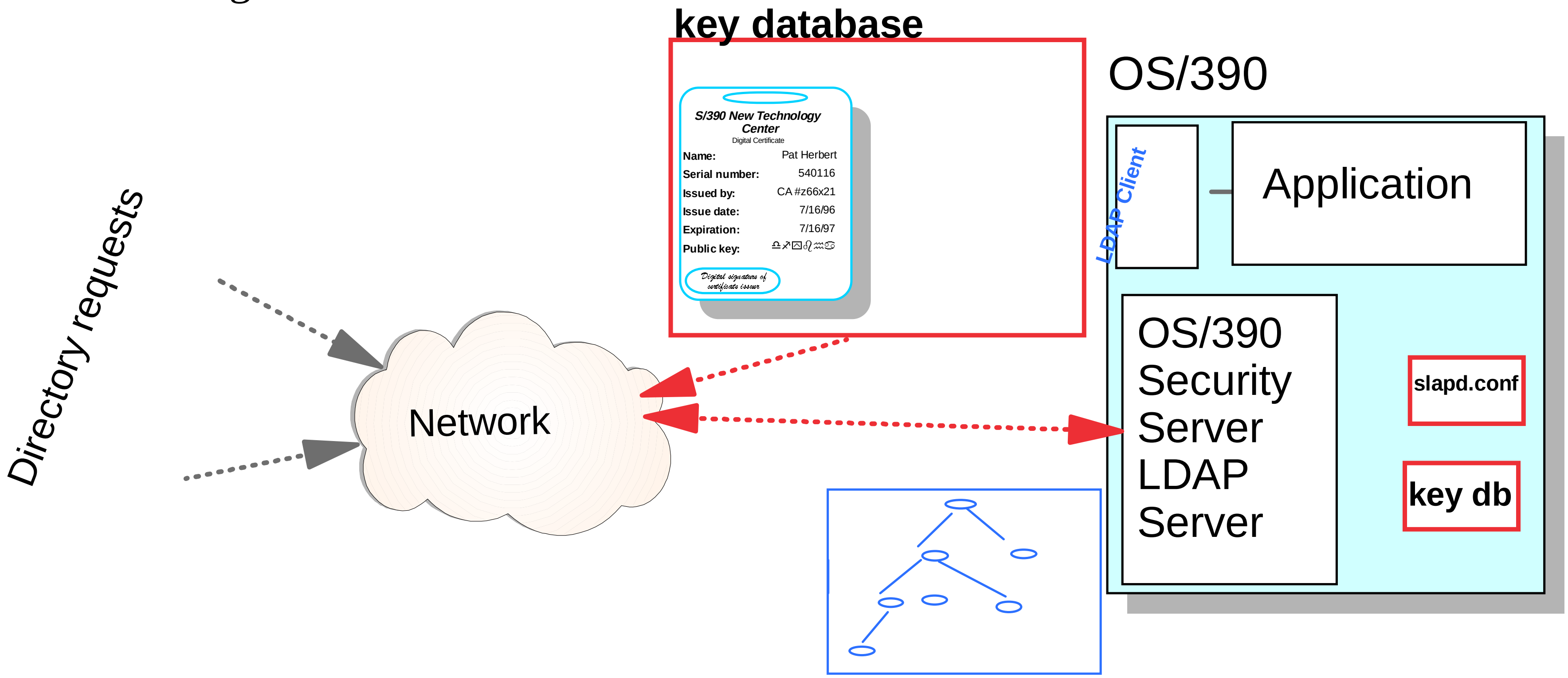


S/390 New Technology Center
Digital Certificate
Name: Pat Herbert
Serial number: 540116
Issued by: CA #z66x21
Issue date: 7/16/96
Expiration: 7/16/97
Public key: ♎♐⊠♌♒♋
Digital signature of certificate issuer

S/390 New Technology Center
Digital Certificate
Name: Pat Herbert
Serial number: 540116
Issued by: CA #z66x21
Issue date: 7/16/96
Expiration: 7/16/97
Public key: ♎♐⊠♌♒♋
Digital signature of certificate issuer

LDAP Client Setup for SSL Support

- Need a Key Database
  - ➤ Can use RACF to keep the certificates
  - ➤ Used to Verify the LDAP Server's Certificate
  - ➤ Must Contain the Signer's Certificate (IMPORT Option)
    - ➤ Either Self-Signed Certificate or the CertAuth's Certificate



S/390 New Technology Center
Digital Certificate

Name: Pat Herbert
Serial number: 540116
Issued by: CA #z66x21
Issue date: 7/16/96
Expiration: 7/16/97
Public key: ♎♐□♌♒♋

Digital signature of certificate issuer

Technology • Connections • Results

GSKKYMAN and Certificates

- OS/390 Crytographic Services, System SSL, includes tool to administer key databases
- Replaced MKKF in OS/390 2.7
- Used for generating Server and Client certificate requests
- Used to store Server and Client certificates for use by Server program and the Client APIs
- Concepts (default certificates, trusted certificates, self-signed certificates)
- System SSL (and LDAP server) supports use of server certificate stored in RACF

Recent LDAP Enhancements on OS/390 - OS/390 R10

- OS/390 V2R10
  - LDAP V3 protocol support (more complete)
    - Schema publication and update
    - Many more syntaxes and matching rules
    - Case Sensitive attributes in distinguished names
    - limited Modify DN support
  - Scalable backend/TDBM
    - Small/fixed DB2 data model allows for tuning
    - Allows multiple DB instances
    - Access control check performance improvements
    - New bulkload utility for TDBM
- z/OS R1
  - LDAP configuration utility
  - Native Authentication

Configuring Password Encryption

- With APAR OW41326 (V2.8), userpassword attribute values can be stored in encrypted form.
  - Encryption uses OCSF, ICSF, and hardware crypto
- Encryption triggered by presence of configuration file option
- Configuration file option: pwencryption, in the database section
  - Only applies to DB2 data store (TDBM or RDBM)
  - Possible configuration values: none(default), crypt, MD5, SHA, DES:keylabel
- Migration utility, db2pwden, will encrypt userpassword values in all existing entries

Features of the z/OS R2 LDAP Server

- z/OS R2
  - LDAP Server
    - concurrent session scalability (up to 64K sessions)
    - access to additional RACF USER profile fields
    - access/update of RACF USER-GROUP connections
    - Kerberos-based authentication (SASL GSSAPI)
  - LDAP Client
    - DNS locate capability for LDAP C/C++ client
    - Client search result caching for LDAP C/C++ client
    - Kerberos-based authentication (SASL GSSAPI)

For More Information

- LDAP RFCs
  - http://sunsite.auc.dk/RFC/rfc/rfc2251.html- rfc2256.html
- OS/390 LDAP Documentation
  - SC24-5861-04 OS/390 Security Server LDAP Server Administration and Usage Guide
    - http://www.s390.ibm.com/ftp/books/os390/pdf/gldaga21.pdf
  - SC24-5878-01 OS/390 Security Server LDAP Client Application Development Guide and Reference
    - http://www.s390.ibm.com/ftp/books/os390/pdf/gld1aa20.pdf