IBM System z – GSE Conference 2008 Leipzig

GS17 - Integrating z/VSE into an Identity Management System

Ingo Franzki, IBM

Ingo Franzki

October 27, 2008

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and / or other counties.

- CICS*
- DB2*
- DB2 Connect
- DB2 Universal Database
- e-business logo*
- Enterprise Storage Server
- HiperSockets
- IBM*
- IBM logo*
- IMS
- Intelligent Miner
- Multiprise*
- MQSeries*
- OS/390*
- S/390*
- SNAP/SHOT*
- Virtual Image Facility
- VM/ESA*
- VSE/ESA
- VisualAge*
- VTAM*
- WebSphere*
- xSeries
- z/Architecture
- z/VM
- z/VSE
- zSeries

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

LINUX is a registered trademark of Linus Torvalds

Tivoli is a trademark of Tivoli Systems Inc.

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

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

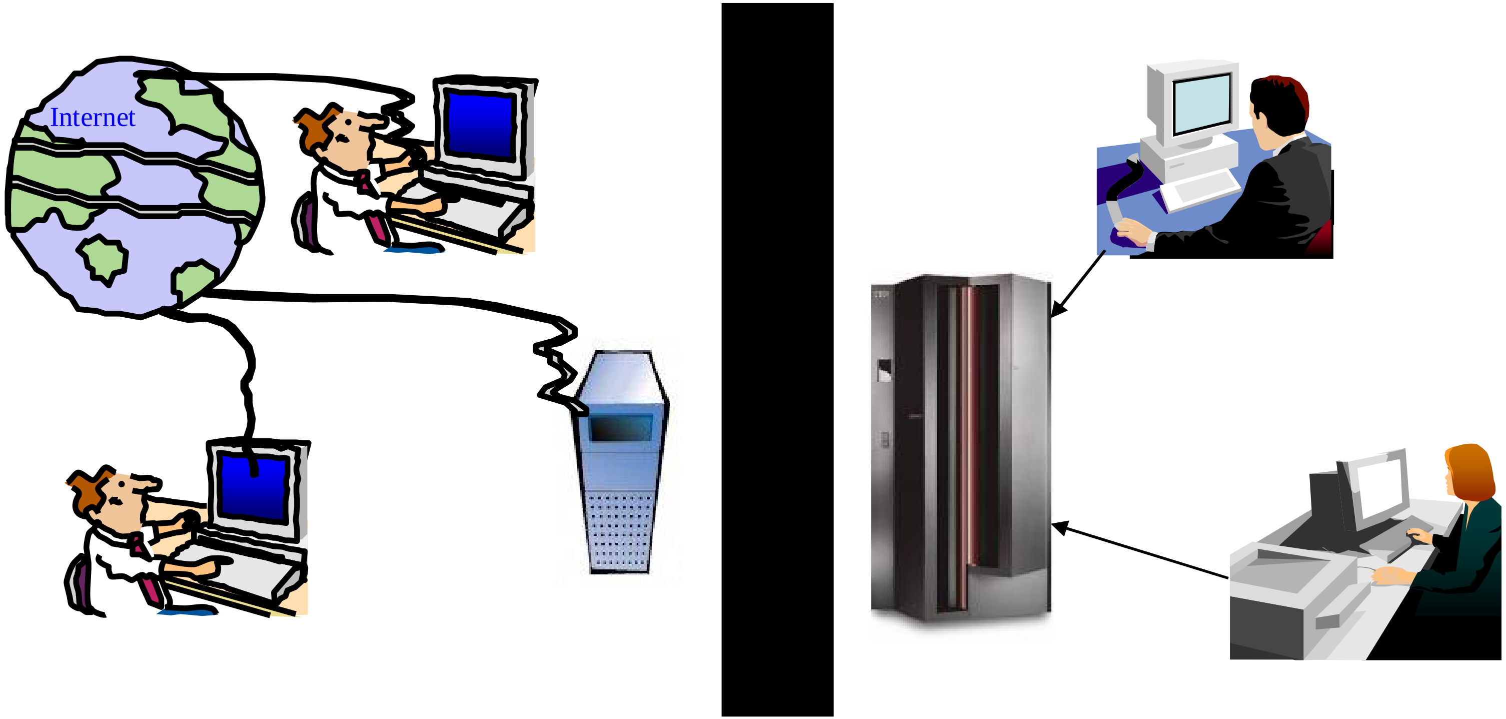
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

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

Intel is a registered trademark of Intel Corporation.

Situation today

- **Separate User-ID Management Systems for z/VSE and the others (Unix, Linux, Windows)**
  - Duplicate User IDs
  - No automatic syncronisation



Situation today - Risks

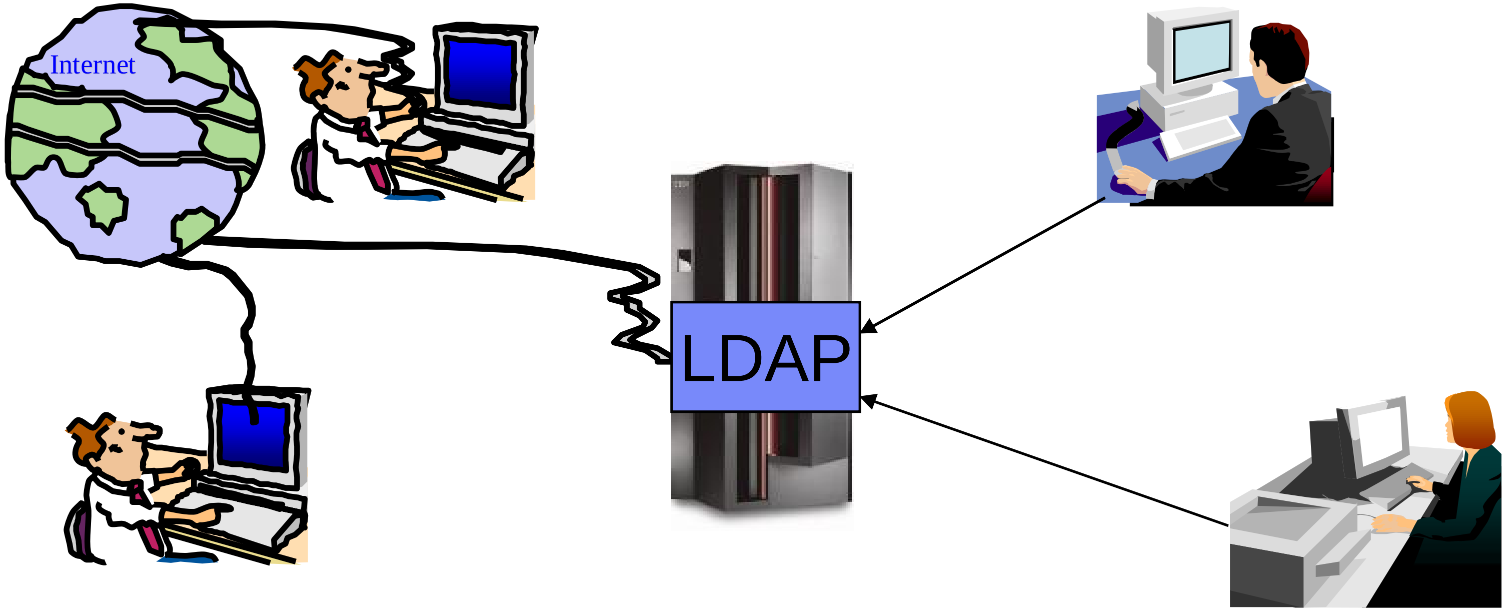
- **User-ID management is very complex if different systems need to be updated**
- **Some User-IDs do not explicitely show who is the owner**
  - e.g. z/VSE 4 Character User-IDs
- **Difficult to enforce corporate policies, like password renewal, auditing, ...**
- **Examples:**
  - If an employee leaves the company
    - Deactive **all** of his User-IDs on **all** systems
  - If an emloyee moves to another department
    - Permissions to access files/programs needs to be adjusted according to his new job on **all** systems
- **If you miss to update one system, the employee (or others) may still have access to confidential data**

Solution: Centralized Identity management

- **Goal:**
  - Only **ONE** place where all Identity related information is stored
    - User-IDs
    - Permissions
    - Groups, Roles
  - All suronding systems access that single Identity Management System
  - Changes to a User-ID (deactivation, modification) automatically affect all systems, without any additional actions
  - Corporate policies can easily be enforced
  - Self servcie Help-Desk can easier be accomplished
    - e.g. Password reset, User-ID unlock, ...

Solution: Centralized Identity management

- **Identity Management Systems typically use a Directory to store ID related information**
  - Protocol to access the directory: **LDAP**



What is LDAP ?

- **The Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP**
  - A directory is a set of objects with similar attributes organized in a logical and hierarchical manner.
    - The most common example is the telephone directory, which consists of a series of names (either of persons or organizations) organized alphabetically, with each name having an address and phone number attached.
- **Due to this basic design (among other factors) LDAP is often used by other services for authentication**
- **An LDAP directory tree often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen.**
- **LDAP deployments today tend to use Domain name system (DNS) names for structuring the topmost levels of the hierarchy.**
- **Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries).**
- **See: Wikipedia: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol**

What is LDAP ?

§ LDAP Terms:

– **Directory**
  - A tree of directory entries.

– **Entry**
  - An entry consists of a set of attributes.
  - Each entry has a unique identifier: its Distinguished Name (DN).

– **Attribute**
  - An attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema

– **Schema**
  - The schema defines the attribute types that directory entries can contain.

– **Distinguished Name**
  - Full qualified name in an LDAP directory tree.
  - Consists of its Relative Distinguished Name (RDN) constructed from some attribute(s) in the entry, followed by the parent entry's DN.
  - Think of the DN as a full filename and the RDN as a relative filename in a folder.
  - Using the DN the object can be identified
  - Example: `uid=104903724,c=de,ou=bluepages,o=ibm.com`

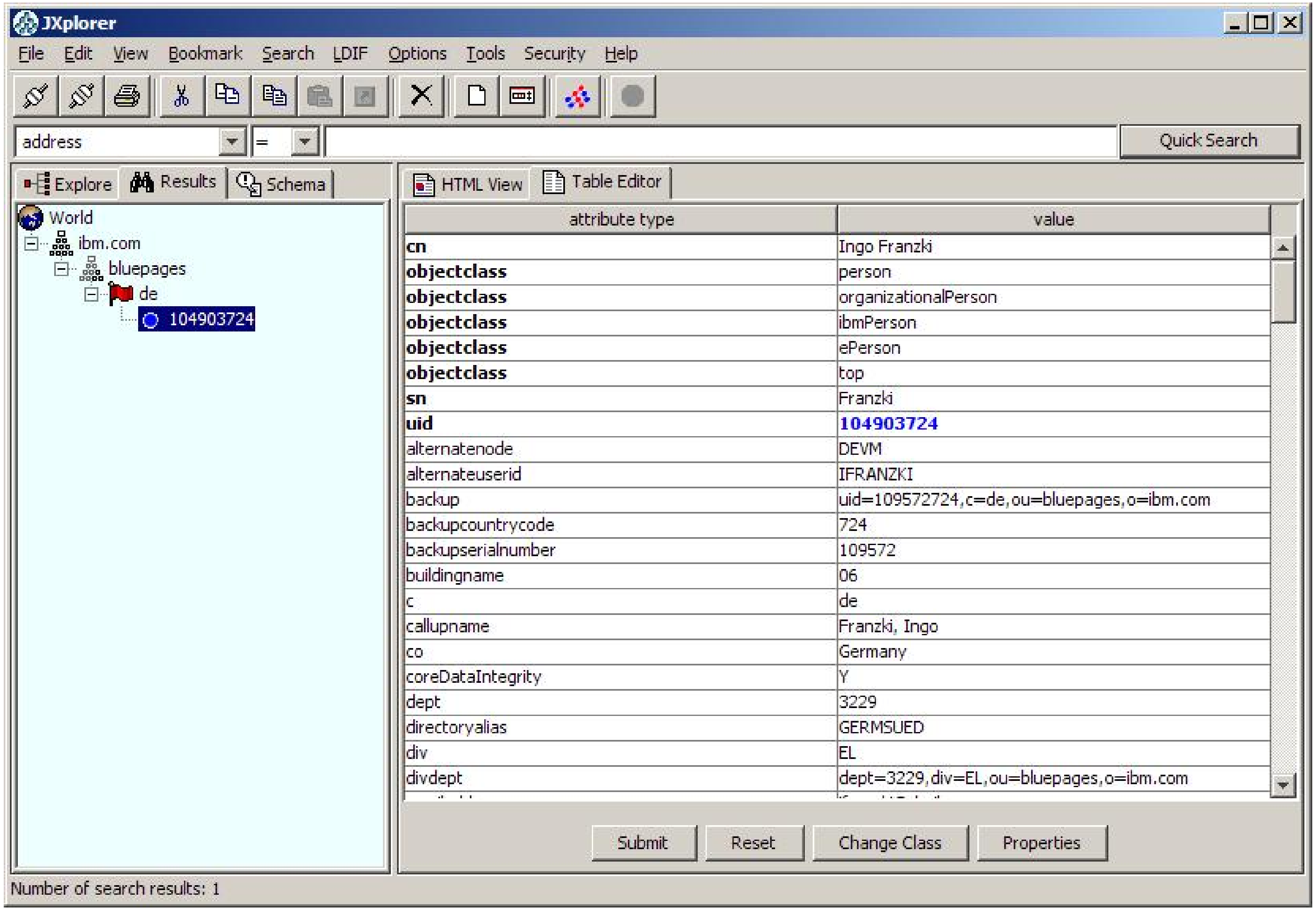
LDAP operations

- **Bind (authenticate)**
  - The Bind operation authenticates the client to the server.
  - Simple Bind can send the user's DN and password in plaintext, so the connection should be protected using Transport Layer Security (TLS).
  - The server typically checks the password against the *userPassword* attribute in the named entry.
  - Anonymous Bind (with empty DN and password) resets the connection to anonymous state.
  - Bind also sets the LDAP protocol version. Normally clients should use LDAPv3, which is the default in the protocol but not always in LDAP libraries

LDAP operations

- **Search**
  - The Search operation is used to both search for and read entries. Its parameters are:
    - **baseObject**
      - The DN (Distinguished Name) of the entry at which to start the search,
    - **scope**
      - BaseObject (search just the named entry, typically used to read one entry), singleLevel (entries immediately below the base DN), or wholeSubtree (the entire subtree starting at the base DN).
    - **filter**
      - How to examine each entry in the scope. E.g. (&(objectClass=person)(|(givenName=John)(mail=john*))) - search for persons who either have given name John or an e-mail address starting with john.
    - **derefAliases**
      - Whether and how to follow alias entries (entries which refer to other entries),
    - **attributes**
      - Which attributes to return in result entries.
    - **sizeLimit, timeLimit**
      - Max number of entries, and max search time.
    - **typesOnly**
      - Return attribute types only, not attribute values.
  - The server returns the matching entries and maybe continuation references (in any order), followed by the final result with the result code.

LDAP Example: IBM Bluepages

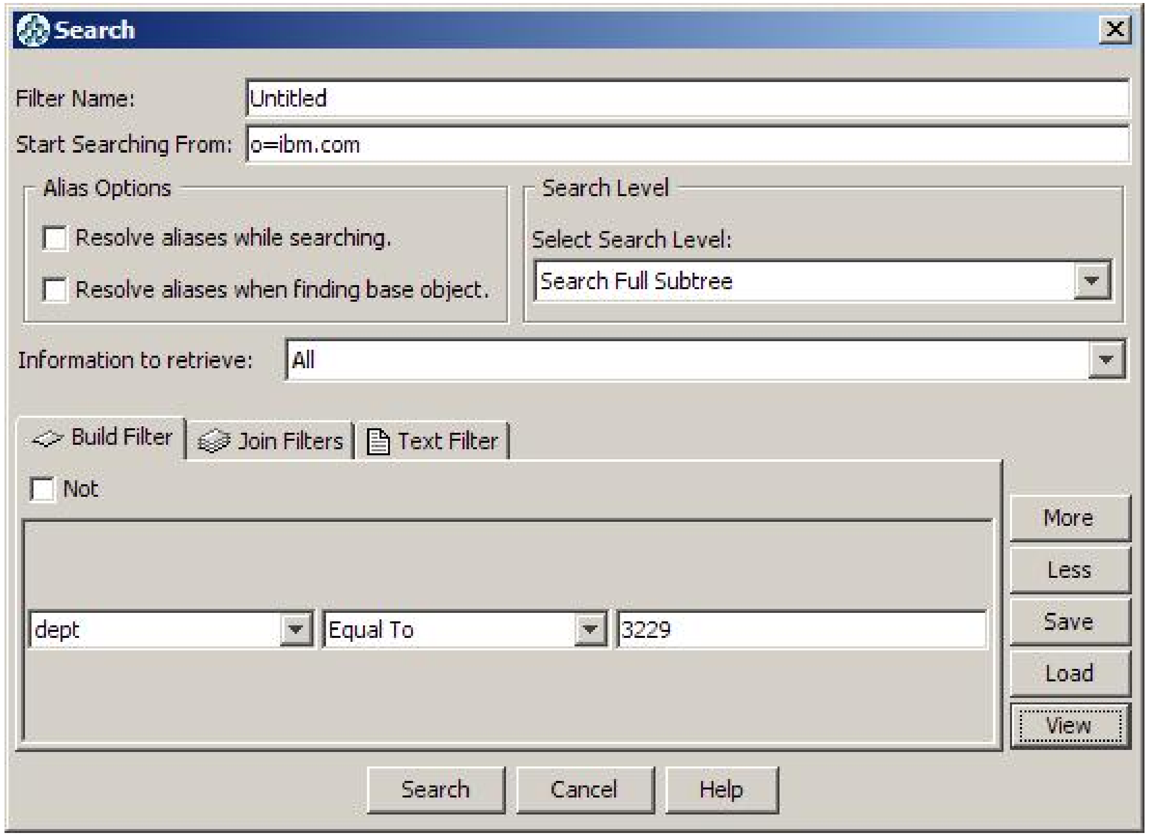


attribute type	value
cn	Ingo Franzki
objectclass	person
objectclass	organizationalPerson
objectclass	ibmPerson
objectclass	ePerson
objectclass	top
sn	Franzki
uid	**104903724**
alternatenode	DEVM
alternateuserid	IFRANZKI
backup	uid=109572724,c=de,ou=bluepages,o=ibm.com
backupcountrycode	724
backupserialnumber	109572
buildingname	06
c	de
callupname	Franzki, Ingo
co	Germany
coreDataIntegrity	Y
dept	3229
directoryalias	GERMSUED
div	EL
divdept	dept=3229,div=EL,ou=bluepages,o=ibm.com

Number of search results: 1

LDAP Example: IBM Bluepages

- **Search for all Entries with „dept=3229“**



Search

Filter Name: Untitled

Start Searching From: o=ibm.com

Alias Options

□ Resolve aliases while searching.

□ Resolve aliases when finding base object.

Search Level

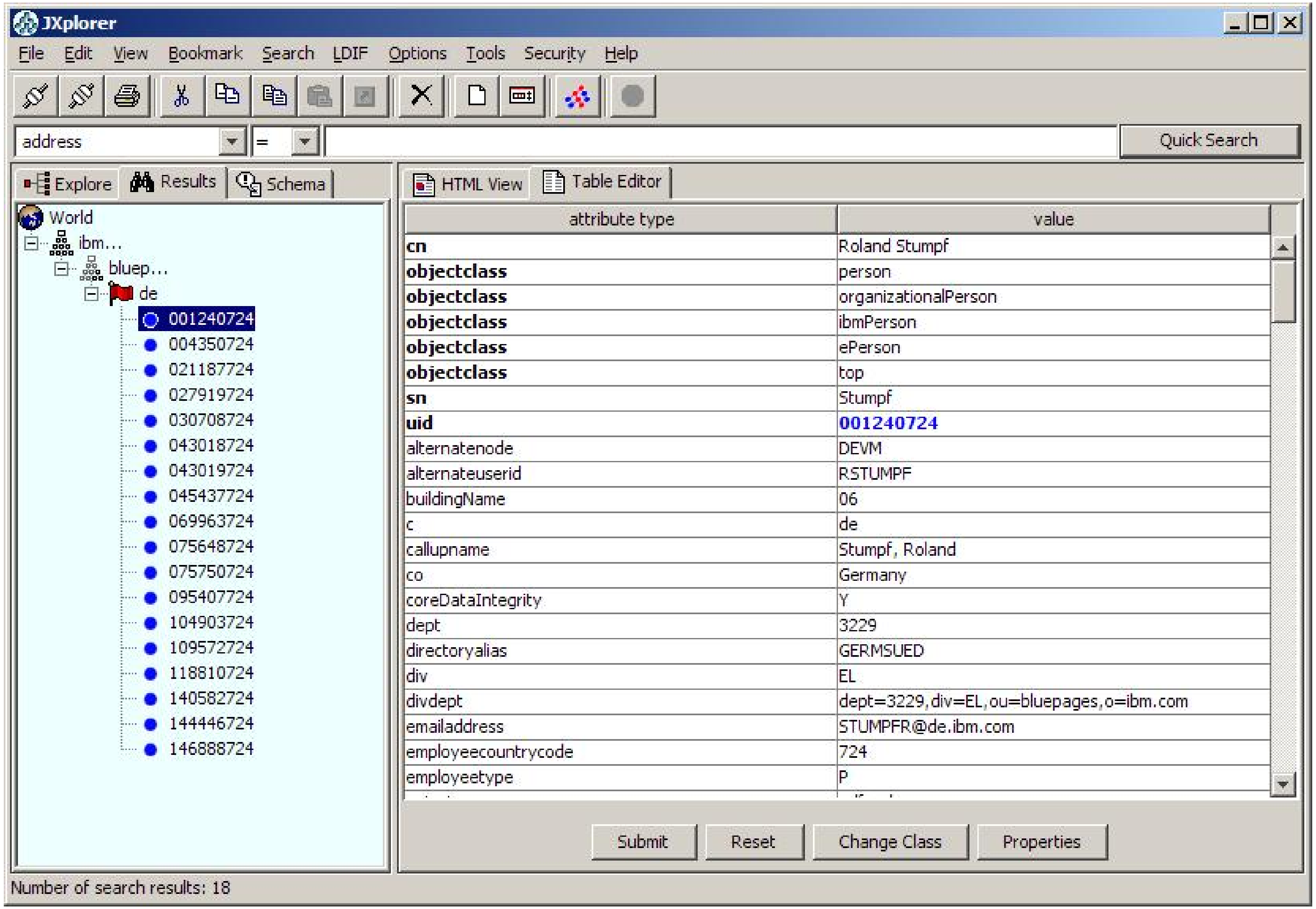
Select Search Level: Search Full Subtree

Information to retrieve: All

□ Not

dept | Equal To | 3229

LDAP Example: IBM Bluepages



- World
  - ibm...
    - bluep...
      - de
        - 001240724
        - 004350724
        - 021187724
        - 027919724
        - 030708724
        - 043018724
        - 043019724
        - 045437724
        - 069963724
        - 075648724
        - 075750724
        - 095407724
        - 104903724
        - 109572724
        - 118810724
        - 140582724
        - 144446724
        - 146888724

attribute type	value
cn	Roland Stumpf
objectclass	person
objectclass	organizationalPerson
objectclass	ibmPerson
objectclass	ePerson
objectclass	top
sn	Stumpf
uid	**001240724**
alternatenode	DEVM
alternateuserid	RSTUMPF
buildingName	06
c	de
callupname	Stumpf, Roland
co	Germany
coreDataIntegrity	Y
dept	3229
directoryalias	GERMSUED
div	EL
divdept	dept=3229,div=EL,ou=bluepages,o=ibm.com
emailaddress	STUMPFR@de.ibm.com
employeecountrycode	724
employeetype	P

Number of search results: 18

LDAP Servers (incomplete list)

- IBM Tivoli Directory Server
- z/VM LDAP Server
- Microsoft Active Directory
- OpenLDAP
- Apache Directory Server
- Apple Open Directory
- CA Directory from CA, Inc. (formerly eTrust Directory)
- Fedora Directory Server (Red Hat Directory Server)
- MXMS, from Atos Origin
- M-Vault, from Isode Limited
- Novell eDirectory
- OneLDAP
- OpenDS
- Oracle Internet Directory
- Penrose - a Java-based Virtual Directory Server.
- Siemens DirX
- SIDVault
- Sun Java System Directory Server
- ....
- (And many more)

z/VSE V4.2 LDAP Signon Support

- **LDAP Signon Support sits on top of any existing Security Manager**
  - It can be used with the Basic Security Manager (BSM)
  - As well as an External Security Manager (ESM)

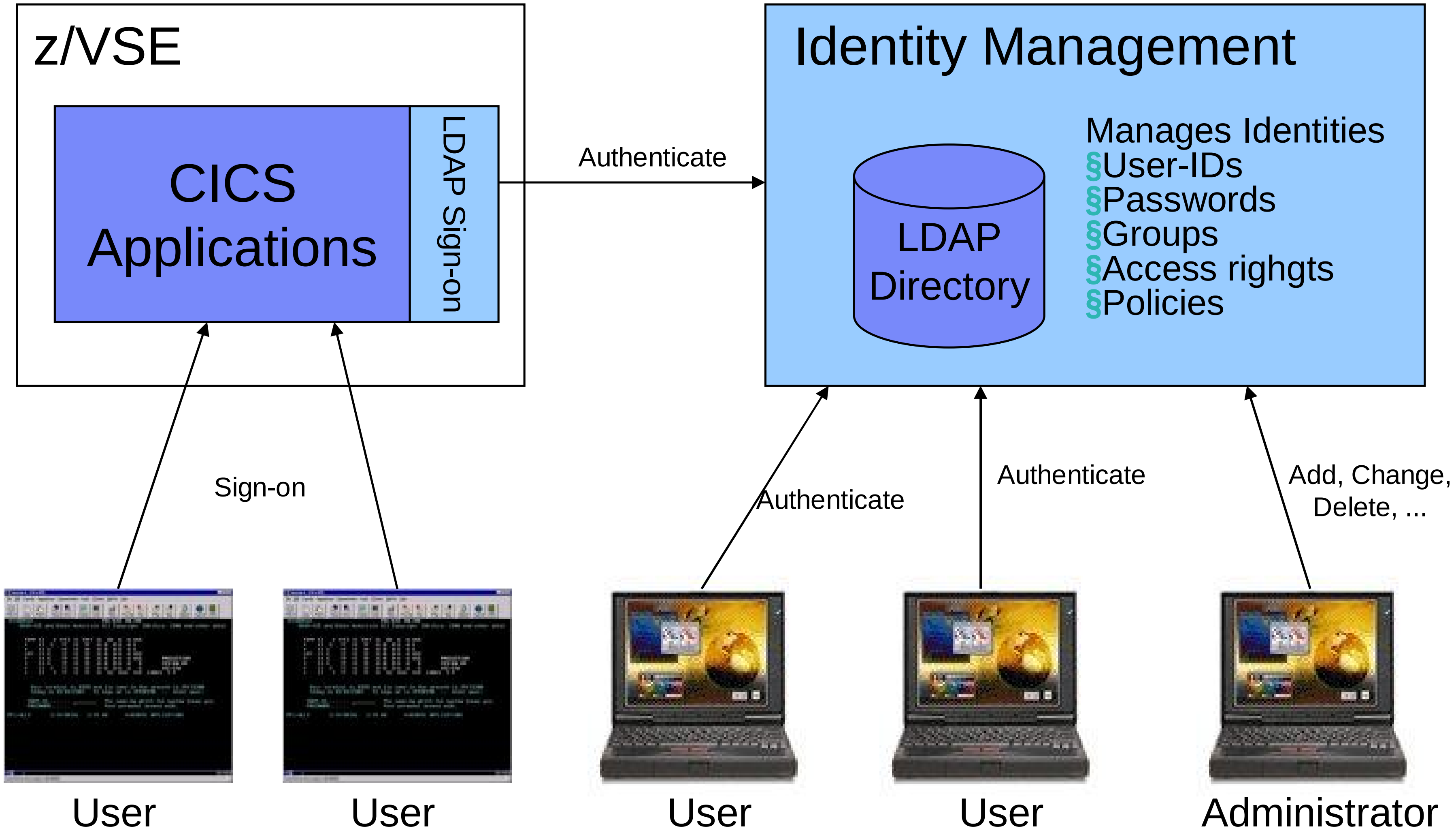
- **Signon process (simplified)**
  1. It first authenticates an user against a remote LDAP server
     - Via LDAP Bind and Search operations
  2. Then it maps the LDAP user to a short VSE user
     - Using a LDAP User Mapping File
  3. Finally passes the short VSE user and password to the existing signon process (BSM or ESM)

- **Currently only available for CICS signon**

z/VSE V4.2 LDAP Signon Support

- **Enables users to sign on z/VSE using a single, comprehensive, corporate-wide 'Identity Management' systems (i.e. IBM Tivoli Identity Manager, etc.)**
- **LDAP user-IDs and passwords can be up to 64 characters. Helps overcome VSE internal limits**
  - 4 character VSE/ICCF user-IDs
  - 4 and 8 character CICS user-IDs
  - up to 8 character Passwords
- **LDAP sign on sits on top of existing z/VSE security manager (i.e. BSM, ESM, etc.)**
- **z/VSE LDAP client can work with common LDAP servers**
  - IBM Tivoli Directory server
  - z/VM LDAP server (with optional RACF repository)
  - OpenLDAP, Apache Directory server, Novell eDirectory, and many others.
- **Potential benefits include improved protection, consistent access rules, ease of use for end-users**

The big picture



z/VSE

CICS Applications

LDAP Sign-on

Authenticate

Identity Management

LDAP Directory

Manages Identities
- User-IDs
- Passwords
- Groups
- Access righgts
- Policies

Sign-on

Authenticate

Authenticate

Add, Change, Delete, ...

User

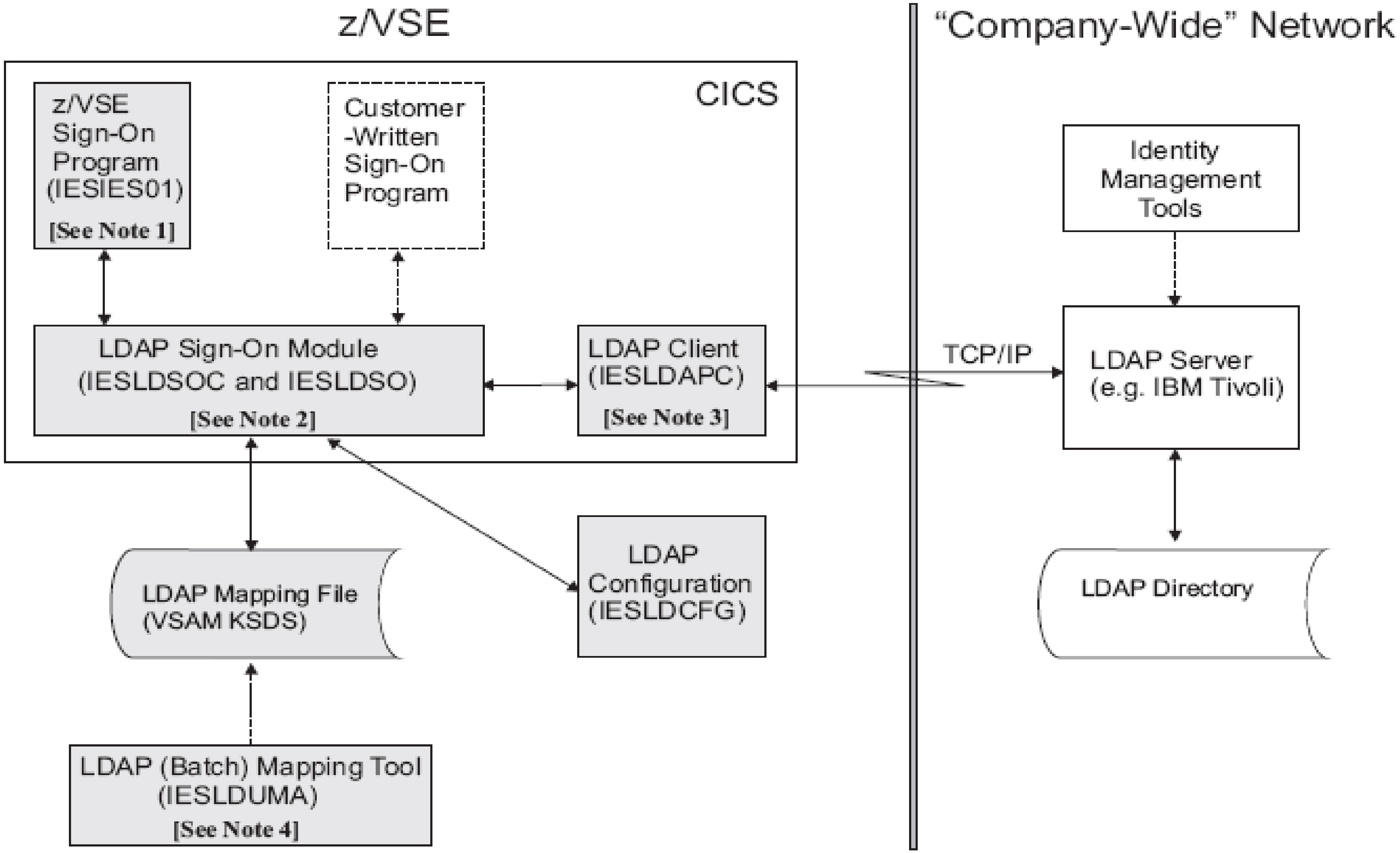
User

User

User

Administrator

z/VSE V4.2 LDAP Signon Support


z/VSE
"Company-Wide" Network
CICS
z/VSE Sign-On Program (IESIES01)
[See Note 1]
Customer -Written Sign-On Program
LDAP Sign-On Module (IESLDSOC and IESLDSO)
[See Note 2]
LDAP Client (IESLDAPC)
[See Note 3]
TCP/IP
Identity Management Tools
LDAP Server (e.g. IBM Tivoli)
LDAP Directory
LDAP Mapping File (VSAM KSDS)
LDAP Configuration (IESLDCFG)
LDAP (Batch) Mapping Tool (IESLDUMA)
[See Note 4]

LDAP User Mapping File

- **VSAM KSDS file used to store the user-ID mappings**
  - LDAP Users & Passwords: up to 64 characters
  - VSE Users & Passwords: up to 8 characters
- **The LDAP mapping file contains:**
  - Records containing user-IDs that are to be used for LDAP-authentication
    - Contain a mapping of a long-user-ID (used in the LDAP environment) to a short-user-ID (used in z/VSE)
    - These user-IDs are referred to as being LDAP-enabled.
  - Records containing user-IDs that are not used for LDAP-authentication (for example, the SYSA user-ID)
    - These user-IDs are referred to as being not LDAP-enabled, and these users can sign on to z/VSE even if the LDAP server is not operational.
- **Maintained using batch tool IESLDUMA**

LDAP Password cache

- **Authentication against a remote LDAP server can be time consuming (requires network communication)**
- **When a user signs on multiple times within a short period of time, it is very unlikely that the LDAP password has changed**
- **If caching is enabled, a shortpath is used to authenticate a user**
  - A password hash (SHA-256) of the last sucessfull signon attempt (LDAP bind) is stored in the User Mapping File
    - There is no way to recover the password from a hash
  - A subsequent signon request builds the password hash, and compares the hash against the stored hash
    - If it is the same, the user has entered the same password
  - A stored password hash has an expiration period. When it is over, a full LDAP signon (LDAP bind) is enforced

LDAP Configuration

- **Per default, LDAP signon is not enabled.**
- **You need to create a configuration to enable LDAP signon support**
  - Use Skeleton SKLDCFG in ICCF library 59
- **Specifies (summary)**
  - DLBL Name of LDAP User Mapping File (default: IESLDUM)
  - IPs or hostnames of one or multiple LDAP Servers
  - Settings for Authentication method (see next foils)
  - Settings for Cache usage and expiration
  - Settings for Secure Socket Layer (SSL)

LDAP Authentication Methods

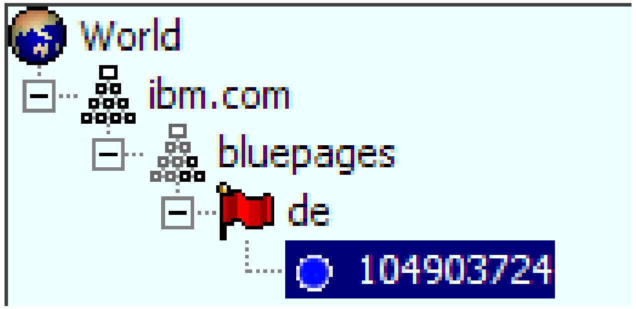
- **LDAP Authentication relies on the LDAP bind operation with distinguished name (DN) and password**

- Direct Authentication:
  - The specified user-ID is used directly for the LDAP bind operation.
  - A pattern is used to build the distinguished name for the bind, e.g. „cn=%u,dc=ibm,dc=com“

- Search Authentication:
  - In case the specified user-ID cannot be used directly for bind.
  - Instead, a LDAP search operation is performed first using the attribute that is specified in the configuration (e.g. „email“).
  - An additional search filter can be specified to further limit the search result, e.g. „dept=3229“
  - The search result’s distinguished name is then used for the LDAP bind operation.

LDAP Authentication Examples with IBM Bluepages

- **LDAP Server: bluepages.ibm.com**


World
ibm.com
bluepages
de
104903724

- **Direct Authentication:**
  - DN would be “**uid=104903724,c=de,ou=bluepages,o=ibm.com**“
  - So pattern would be „**uid=%u,c=de,ou=bluepages,o=ibm.com**“
  - LDAP User ID would be IBM personal number: „**104903724**“
  - LDAP Bind will be performed with „**uid=104903724,c=de,ou=bluepages,o=ibm.com“** and the specified password

LDAP Authentication Examples with IBM Bluepages

§ Search Authentication:

- Every person entry has an attribute named „**email**“ that contains the user‘s email address
- BaseDN for search (start of search) would be „**ou=bluepages,o=ibm.com**“
- Additional search filter either empty (no filter) or „**dept=3229**“ if search should be limited to persons in department 3229
- LDAP User ID would be email address: „**ifranzki@de.ibm.com**“
- LDAP Search will be:
  - Start at „**ou=bluepages,o=ibm.com“** and look for entries where **email=ifranzki@de.ibm.com & dept=3229**
  - Result will be just me, i.e. My DN: **uid=104903724,c=de,ou=bluepages,o=ibm.com**
- LDAP Bind will be performed with „**uid=104903724,c=de,ou=bluepages,o=ibm.com“** and the specified password

Using your own CICS Sign-on program

- **The Interactive Interface signon program (IESIES01) has been adapted to support LDAP authentication**
  - If LDAP authentication is configured and enabled, it will automatically show longer fields for userid and password

- **If customers use their own sign-on program, they need to adapt it to use LDAP sign-on support:**
  - Enlarge fields in screen (BMS map) for userid and password
  - Support case sensitive input
  - Call LDAP Sign-on Program IESLDSOC to perform LDAP authentication
    - Using EXEC CICS LINK with COMMAREA (see Admin Guide)
  - Sample CICS Sign-on Program supporting LDAP is available on request (zvse@de.ibm.com)

Restrictions

- **No support for using long-user-IDs in the ID statement within batch jobs**
  - ID statements can only use a short-user-ID and short-password (a “z/VSE” user-ID and password).
- **LDAP sign-on is only possible using a CICS sign-on panel.**
  - The z/VSE-provided LDAP sign-on panel (IUI signon)
  - A customer-written sign-on panel.
- **Only LDAP Authentication (using Bind) is supported**
  - Kerberous authentication (often used by MS Active Directory) is not supported

LDAP Tools and Documentation

- **LDAP Browser**
  - JXplorer (http://www.jxplorer.org/)
- **z/VSE Manuals:**
  - **Planning:** Subchapter in chapter 18. Security and Encryption Support: LDAP Sign-On Support
  - **Administration:** Chapter 45. Maintaining User Profiles in an LDAP Environment
- **Internet:**
  - Wikipedia: http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Questions ?