

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

Jordan e.Government Enterprise Directory Scope

Final Report

**Deliverable for ICTI Component, Task No. 431.4.10
Contract No. 278-C-00-02-00201-00**

June 2002

This report was prepared by Paul MacLean, in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan

0 Document Control

Table of Contents

0	DOCUMENT CONTROL	3
0.1	Document History	5
0.2	Changes From Last Issue.....	5
0.3	Acknowledgements	5
0.4	Distribution List.....	5
0.5	Referenced Documents.....	5
0.6	Abbreviations	5
0.7	Glossary.....	6
1	INTRODUCTION	8
1.1	Purpose	8
1.2	Scope	8
2	ROLES OF DIRECTORIES	9
2.1	Microsoft Active Directory	9
3	TIME FRAME FOR AVAILABILITY OF DIRECTORY SERVICES.....	10
3.1	Application Directory	10
3.2	White Pages	10
3.2.1	Exchange 2000 GAL.....	10
3.2.2	Personnel Directory.....	11
3.2.3	Organizational Directory.....	11
3.3	Network Operating System Directory	11
3.4	E- Commerce Directory.....	12
3.5	Multi-Language Support	12
3.5.1	Translate user information.	12
3.5.2	Store Multi Value user information	12
3.6	Dedicated GC for Portal Searches	13
4	ACTIVE DIRECTORY DOMAIN STRUCTURE	14
4.1	Place Holder Domain	14
4.2	Addition of Child Domains	14
4.3	Multiple Forests / Multiple Exchange Organization	15

Table of Figures

Figure 1 – Ministry eMail Users	10
Figure 2 – Single Forest / Single Organization	14

0.1 Document History

Version	Status	Approved by	Date
0.1	Draft	N/A	17 June 2002

0.2 Changes From Last Issue

Ver	Date Updated	Revision Author	Summary of Major Changes Made	Reviewed By	Review Date
0.1	10 June 2002	Paul MacLean	Initial document created and internally reviewed.	Paul Williams Allan Gormley	17 June 2002
1.0	22 July 2002	Paul MacLean	Update header ,footer and copy right information	Tariq Mahmood	24 July 2002

0.3 Acknowledgements

N/A

0.4 Distribution List

Allan Gormley	EDS
Kendall Lott	EDS
Sherry Yousef	AMIR
Mahmoud Ali Khasawneh	MoICT
Abed Shamlawi	AMIR

0.5 Referenced Documents

Number	Title	Reference	Note
1.			
2.			
3.			
4.			
5.			

0.6 Abbreviations

GOJ	Government of Jordan
MoICT	Ministry of Information, Communications and Technology (previously MoPC).
MDS	Messaging and Directory Services
AD	Active Directory
GAL	Global Address List
GC	Global Catalog

0.7 Glossary

•Active Directory (AD)

AD is the directory service used in Windows 2000. The directory service stores information about all the resources on a network, such as users, groups, printers, files and applications. It also provides the services to make the information available. This information is stored in an hierarchical structure as objects. Each object has attributes such as a name, phone number, or email address.

•Domain

The basic unit of organization and security within AD.

•Domain Controller (DC)

A server that can authenticate users for a domain. There must be at least one domain controller in each domain within the forest. Each domain controller holds a complete replica of the domain-naming context that the server is in and a complete replica of the configuration and schema naming contexts for the forest. A domain controller can be promoted and demoted through the Dcpromo utility.

•Schema

The AD Schema consists of different objects, or components, that control the classes and attributes maintained by AD. Modifying these components changes the definitions of the objects and directly affects how AD operates. Attributes can be marked for inclusion in the GC, however this causes all objects in the AD to be replicated out to the GCs, thereby impacting network traffic.

•Global Catalog (GC)

A server that holds a complete replica of the configuration and schema naming contexts for the forest, a complete replica of the domain naming context in which the server is installed, and a partial replica of all other domains in the forest. The Global Catalog knows about every object in the forest and has representations for them in its directory, however, it may not know about all attributes (such as job title and physical address) for objects in other domains. The attributes that are tagged for replication to the Global Catalog are assigned through the Active Directory Schema Manager Microsoft Management Console (MMC) snap-in. There is only one *policy* for Global Catalog attribute replication in the forest. A Global Catalog will listen on port 3268 for LDAP queries (that are global to the forest), and port 389, which standard domain controllers use (for local domain queries). A domain controller can be made into a Global Catalog (and vice versa) by selecting or deselecting a check box in the Active Directory Sites and Services MMC snap-in.

•Organizational Unit

An OU is a container; it can hold objects like users, computers and groups. It is also a security boundary in that it can have multiple policies applied to it. It makes up the most significant administrative component of the domain.

•Tree

A collection of domains that have a contiguous namespace, such as *microsoft.com*, *dog.microsoft.com* and *cat.microsoft.com*. Domains within the forest that do not have the same hierarchical domain name are located in a different domain tree. A *disjoint namespace* is the term used to describe the relationship between different domain trees in the forest

•Forest

A collection of domains and domain trees. The implicit name of the forest is the name of the first domain installed. All domain controllers within a forest share the same configuration and schema naming contexts. To join an existing forest, the Dcpromo utility is used. The first domain within the forest cannot be removed

•Site

A collection of IP subnets. All computers that are in the same site have high-speed connectivity—local area network (LAN) speeds—with one another. Multiple sites may exist within a single domain, and conversely, a single site may span multiple domains.

User Principal Name (UPN)

This is a unique method of identifying each user across a forest and typically equates to an email address like *rooster@hoosierfarm.com*. A UPN allows the underlying domain structure and complexity to be hidden from

users; for example, although 50 domains may exist within a forest, users would seamlessly log on as if they were in the same domain.

LDAP

A standards-based protocol that can be used to interact with conformant directory services. These include: Windows 2000 AD; MS Exchange Server 2000; Windows NT4.0 And 3.51; NetWare 3.x bindery based system; Netware and IntraNetware 4.x and 5.x NDS; Netscape Commerce Server; Netscape Directory Server 1.0; IBM Lotus Notes; MS Web Based Enterprise Management WBEM; MS internet Information Server (IIS); MS Commercial Internet Systems address Book Server; and MS Site Server. LDAP was developed by Tim Howes and the University of Michigan.

1 Introduction

1.1 Purpose

In support of the Government of Jordan's move towards becoming an electronic Government there is an agreed strategy to provide a corporate directory and an enterprise messaging service. These services will be made available to all registered Government employees and applications. The optimal solution will be located in a data centre and centrally administered. As stated Directory Services is an important piece of the GOJ e Government philosophy. This document will describe some of the functions of the Enterprise Directory and try to provide options and offer best practices where necessary.

1.2 Scope

This document is will recommend the scope of the Enterprise Directory for the initial October time frame for deployment of the Enterprise eMail system / SGN rollout and identify future functionality to be deployed.

2 Roles Of Directories

An Enterprise Directory is a directory that can fill many roles at one time. The 5 major roles an Enterprise Directory needs to fill are:

- Application Directories
 - Manage application specific user authorization eMail , SQL, etc
- White Pages Directory
 - A simple place to go to find people, phone numbers, addresses etc.
- Network Operating System Directory
 - Users and resource access information
- E- Commerce Directories
 - External User Profile information stored in a directory

These are all functions that GOJ is looking to provide to employees, vendors, and citizens.

2.1 Microsoft Active Directory

Microsoft Active Directory is the directory of choice for the Enterprise Directory. It is arguably the best in breed in all of the directory roles described above. Microsoft Active Directory is Built on industry standards such as LDAP, Kerberos and PKI.

3 Time frame for Availability of Directory Services

In October 2002 GOJ will be rolling out The Secure Government Network (SGN), Centralized Enterprise Exchange 2000 mail system, and a Government Portal. These deliverables will require the following functionality: Application Directory, White Pages and to some extent The Network operating system Directory.

3.1 Application Directory

Exchange 2000 requires the user to have a UserID, Mailbox and access rights. All pertinent information, such as mailbox location, can be stored in the Active directory User record. User rights will be assigned on a roles and business rules basis. This means that Groups will be created with roles associated to them such as *Exchange Administrator* or *SQL user*. Other applications such as SQL can query the AD to authenticate the user and allow him access based on the groups he belongs to. Creation of roles and groups should be done on a committee basis to ensure that only roles and groups that are absolutely required are created.

The Government Portal, as described by DevIS, will authenticate users by querying the Active Directory and allowing access rights as assigned in the Active Directory. The initial directory functions of the Government Portal will not require authentication. Future Government Portal functionality may require authentication.

3.2 White Pages

3.2.1 Exchange 2000 GAL

Exchange 2000 provides a Global Address List (GAL), which is a directory of all users and contacts in the Exchange system. This allows a user to find an eMail address, physical address or phone number of any user in the Exchange system. The initial deployment will consist of six ministries from October through December 2002. These Ministries comprise of approximately 700 users.

Ministry	Current eMail Users	Initial eMail Users	Current eMail System
Ministry of Information and Communication Technology (MOICT)	70	70	Exchange 5.5
Ministry of Public Works and Housing (MPWH)	3	30	Dial-up
Ministry of Industry and Trade (MIT)	108	108	SendMail
Ministry of Planning (MOP)	180	180	SendMail
Prime Ministry (PM)	120	120	SendMail
Ministry of Finance (MOF)	22	30	SendMail

Figure 1 – Ministry eMail Users

This means that only these users will exist in the GAL and the GAL will grow incrementally as ministries join the Exchange system. Administrators will initially add the employee information but the individual employee will be responsible for keeping his information such as Telephone number and address updated.

GOJ needs to decide whether they want to collect user data for all other employees in the GOJ and enter them in the Exchange 2000 system as contact information. This would provide the pertinent information for GOJ employees in the GAL but not provide mailboxes. This would allow a GOJ employee who is an Exchange user to look up any other GOJ employee in the GAL. He would only be able to send Contacts email if their current email information is collected and entered in the contact information. As Ministries join the Exchange system the contacts will be changed to user records and the user will be assigned a

mailbox. Collection, entry and maintenance of this information are a large task as there are approximately 100,000 GOJ employees. The directory is only as good as the information entered in it. This would also allow non-Exchange employees and citizens to access information by using the web based personnel directory. This personnel directory is discussed further below.

It is not recommended that all 100,00 entries be in the Exchange Gal on day one of the rollout. It is recommended that the Directory grow gradually and that the first couple of months be used as a pilot phase.

3.2.2 Personnel Directory

The Personnel Directory is one function of the Government Portal that is to be available in October 2002. This Personnel Directory is a G2G (or G2Employee) directory only. The G2G (or G2Employee) users will be able to search the Active Directory and identify individual government employees by organization, phone number, email, or physical address. This is only a browse function. The Active Directory will not be updated from the Government Portal.

Even though this is a browse only function the search of the directory needs to be tightly controlled from the Portal. For example, wild card searches should not be allowed and the number of items returned should be limited in order to ensure that Denial of Service (DOS) does not occur.

According to DevIS the Personnel Directory will only be available to users who are connected to the SGN. I agree with this assumption, otherwise there would have to be a way to authenticate a public user through the Internet and differentiate between citizens and Government Employees. While this functionality will be available in the future, it is unadvisable to complicate the rollout of the Exchange 2000 system and add all the extraneous UserIDs just to be able to look up employees. It is recommended to build the directory incrementally at least through the pilot phase to ensure a successful rollout. If the Users were added initially there would be issues with keeping information up to date, and keeping passwords valid.

3.2.3 Organizational Directory

The Organizational Directory is another function of the Government Portal that is to be available in October 2002. The enterprise directory will provide access to contact information for GOJ organizational units. This Organizational Directory is a G2B or G2C directory only. The G2B or G2C users will be able to search the Active Directory and identify Governmental Ministries/ Agencies by phone number, email, or physical address. This is only a browse function. The Active Directory will not be updated from the Government Portal.

Even though this is a browse only function the search of the directory needs to be tightly controlled from the Portal. For example, wild card searches should not be allowed and the number of items returned should be limited in order to ensure that Denial of Service (DOS) does not occur. Citizens would not require an UserID to use the Organizational Directory functionality.

According to DevIS the Organizational Directory will be available to users from the public Internet and the users who are connected to the SGN.

3.3 Network Operating System Directory

By default Active Directory is a Network Operating System Directory. It contains information on users and resources. It provides security and controls many aspects of the File/Print environment. It can also provide a high level of Desktop security and configuration when teamed with Windows 2000 Professional or Windows XP professional desktop.

Currently MOICT is the only Ministry, of the 6 ministries identified for the initial rollout that has a Windows NT infrastructure. All other ministries have either a Unix infrastructure or no infrastructure at all. For the initial rollout it is recommended that AD be rolled out for eMail purposes only to all Ministries except MOICT. Eventually a Directory Services project should be undertaken for each ministry to decide what level of directory services would be required, whether they will use the administrative and security policy of the default Active Directory deployed with Exchange 2000 or whether they would require their

own domain or forest. Political and security reasons would be the main reasons for a ministry to require its own domain or forest.

3.4 E- Commerce Directory

An E-Commerce directory is a directory that contains external users. It would generally be used to authenticate external users and to provide a user with a personalized environment for their web experience. It would contain personalized user profile information. It should be scalable for millions of users because potentially all citizens could have their own ID on this system. This Directory could be Microsoft Active Directory, but because Active directory is a NOS directory and contains elements such as HOME Directory and Login script; there may be directories such as SUN's that are a better fit for an E-Commerce directory. One advantage of this E-Commerce directory being a Microsoft Active Directory would be the expertise that GOJ would have garnered from using Active Directory internally. If the E-Commerce directory is decided to be an Active directory, It should be a totally separate External facing directory in a separate forest containing only citizens and Businesses. It should not contain employee data. As to date I do not recommend this functionality being deployed in October 2002. There are not any Portal function that have been identified that will require this functionality in October 2002.

3.5 Multi-Language Support

One issue with the Portal based directory searches described by DevIS is the requirement to be able to display the content in either English or Arabic. Because Microsoft Active Directory is UNICODE based, it has the ability to store either Arabic or English characters. Out of the box AD can only store a single instance of a field, this field can be stored in either English or Arabic not both. There are two fields that must be stored in English in the Active Directory, User Name and Logon Name. User Name, Address, Ministry Name, Full name, and other fields will be required in both languages. There are two ways to handle this dilemma, translation or storing multiple instances of the user information.

3.5.1 Translate user information.

One solution would be to Store the content once in the Active Directory (in English) and then have the Portal translate the data to Arabic when a user requests this information in Arabic. There are numerous third party Translation products that can be used to quickly accomplish this task. The major problem with translation is that translation algorithms are usually character based not word based. This means that the translation may not accurately translate the words correctly. Names are also more difficult to translate than Normal words. The advantage to translation is that the content is stored in one place and is easier to enter and maintain.

3.5.2 Store Multi Value user information

The recommended way to fulfill this requirement would be to store the user information such as: Display Name, Telephone number, and address in both English and Arabic. There are two ways to do this. One would be to have two separate directories, one with content stored in English and the other directory with the content stored in Arabic. The portal would have to query the appropriate directory when a search request is made.

The second way to handle this requirement would be to expand the Active directory schema to include a second instance of the User information fields. This second method is a cleaner method because you would not have to implement an entire directory infrastructure just to store the user field contents in 2 languages. One drawback of extending the Active directory schema is that you would not be able to use the Active Directory MMC to enter and maintain the new fields added to the schema. You would have to either modify the MMC dlls to access these fields or use a third party product such as Aelita's Enterprise Directory Manager. Any changes to the MMC could potentially be over written any time a service pack or any Microsoft software is installed on the server.

The only way to control that both the English and Arabic content is entered and maintain would be strict adherence to Administration policy by the people responsible for creation and maintenance of UserIDs.

3.6 Dedicated GC for Portal Searches

In order to ensure the best possible response time for both internal Exchange 2000 users and the Portal users, it is recommended that a dedicated GC be deployed for the portal directory searches.

4 Active Directory Domain Structure

The Government of Jordan will be deploying a Single AD forest / Single Exchange Organization infrastructure for the first six ministries to be deployed beginning October 20002.

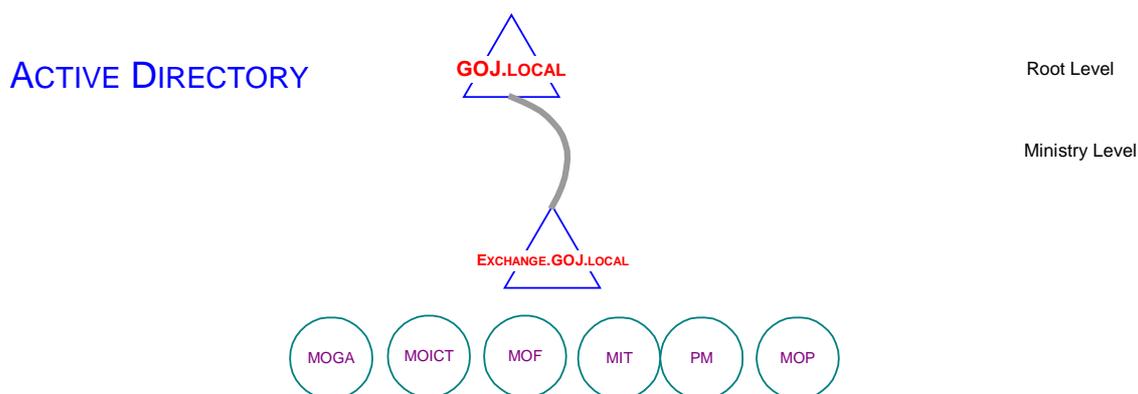


Figure 2 – Single Forest / Single Organization

4.1 Place Holder Domain

The AD domain structure will utilize a Place Holder domain structure. This will allow the environment to be more dynamic with the additions of new organizational units or domains as ministries come on line. By creating the Root Domain as a placeholder or “Empty” domain, this allows the ability to add Child Domains to the tree to accommodate ministries that want more control of their infrastructure.

Another primary reason for implementing empty forest roots is to secure, as much as possible, access to the Enterprise Admins and Schema Admins groups. With a placeholder domain, the forest root doesn’t host any user or group objects and is administered by only a small number of administrators. The child domains are the primary containers for Active Directory objects and the majority of the day-to-day administration takes place in these child domains. With this approach the domain administrators in the forest rarely touch the forest root domain and you can easily manage control over the members of the Enterprise Admins group.

For the Initial six ministries, OU’s will be created under the Exchange.GOJ.Local AD domain for each ministry. All users in these ministries will reside in the Ministries User container. Each users email address will be based on the OU the user belongs to. For example MOICT users SMTP address would be USERID@moict.gov.jo and MOP users would be USERID@mop.gov.jo.

4.2 Addition of Child Domains

If a ministry is further along in its Directory Services planning and wants more control of its users, directory and Infrastructure a Child domain Such Ministry of Finance (MOF.GOJ.local) would be added. MOF would still be utilizing the centralized Exchange servers located in the data centre. Their email domain would remain USERID@MOF.gov.jo

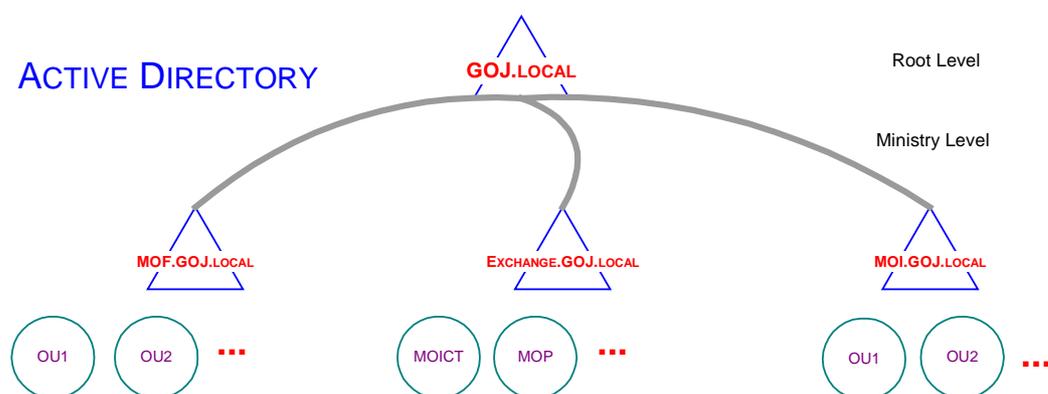


Figure 3 – Additional Child Domains

The Ministry of Interior (MOI.Jordan.local), wants more control of their directory services and email environment. They have stricter Security policy and different Backup policy. They could have their own Local Exchange server, but it still belongs to the one centralized Exchange organization. Their email Domain is USERID@MOI.gov.jo

This Single Forest / Multiple domain architecture supports the following functionality.

- **Supports a decentralized administration model:** While GOJ will be utilizing a centralized support Model, if the need arises, this model is highly adaptable to a decentralized support model. Members of the Domain Admins Group in each domain only have authority over the local domain. Still requires coordination among Domain admin groups.
- **Supports multiple domain security policy:** Security policy settings are only available at the Domain level. Although you can set different security policies, GOJ should enforce a global security policy. That Ministries would have to show clear reasoning for their desire to create a different security policy and therefore a new Domain.
- **Supports domain and/or OU administrative delegation:** AD supports the capability to delegate authority for specific administrative functions. This can be done at either the Domain or OU level. In this model delegation can be set at either level.
- **Replication traffic isolation:** Replication is isolated between domain controllers within the same domain. Forest wide information such as schema, global catalog, and configuration container are replicated between domains, but this is generally a small percentage of the domain replication.
- **User authentication:** Through Kerberos trusts, domain users can be authenticated through any domain in the tree.
- **Cannot “demote” a domain:** A child domain cannot be “demoted” to an OU if it is not necessary. But OU’s can be made into domains. You need to be careful when making the decision to create a child domain.

4.3 Multiple Forests / Multiple Exchange Organization

Due to the diverse security requirements of the GOJ ministries, there is the potential for a Ministry such as the Ministry of Defence to require isolation of its Active Directory and Messaging systems. This model provides the security boundaries required for this type of isolation. However, for this Ministry to participate in inter forest user collaboration with the users in the GOJ.Local Forest, directory and data replication is required between the AD forests and the Exchange organizations. Tools required for this type of replication would be Microsoft Metadirectory Service (MMS) and the interorg replication tool.

ACTIVE DIRECTORY

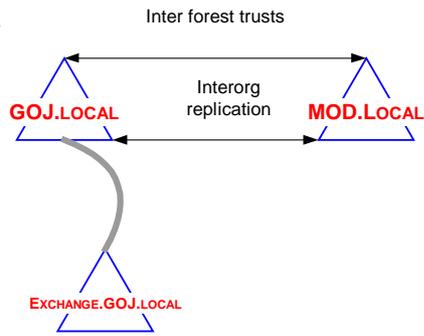


Figure 4 – Multi Forest / Multi Organization