EPIC

Planning Guide

VM-0001-02

About this book:

This book describes the information that users need to consider before they install and configure EPIC.

Who this book is for:

The book is intended for readers with some knowledge of EPIC and a general understanding of computer systems.

What you need to use this book:

An understanding of the concepts described in the VM-0001-01 System Overview is required.

Related Publications:

VM-0001-01 System Overview

Table of Contents

1 Introduction

This publication describes the hardware and software requirements for EPIC (Enterprise Process Integration Controller) and also the planning, configuring and implementation decisions that need to be considered before the installation.

This publication covers the following topics:

- Hardware and software requirements to install and run EPIC on your network
- EPIC's database, proxy and implementation options and configurations
- Client and server deployment describes the different roles each client and server offers, and the applicability of each application to the end user
- System security deployment strategies and security options to ensure your system remains secure
- Internal system integration options available between your internal systems and EPIC, and how to streamline the integration
- Workflow configurations describes how workflows can be designed to meet your business requirements
- Identifying your trading partner requirements and prerequisites to support EPIC's range of communication and network protocols

2 Hardware and Software Requirements

2.1 Software

To install and run EPIC, you will require Windows XP SP2, Windows Vista, Windows Server 2003 SP2, Windows Server 2008 or Windows 7 with Internet Explorer 6 or above already installed.

The EPIC software architecture allows multiple clients to be installed throughout your corporate network, whilst still connecting to the same central server. However, the client/server architecture is independent of the underlying operating system and so, if required, different operating systems can be used in the deployment of EPIC.

The EPIC installation will also install the following pre-requisites if they are not already present on the machine:

- Windows Installer 4.5
- Microsoft Visual C++ 2008 Redistributable Package
- Microsoft SQL Server 2008 Express Edition (optional)

In addition to these pre-requisites, the Microsoft .NET Framework Version 4 is also required. This is not installed by EPIC, so will need to be present prior to installation.

Microsoft's .NET Framework has been designed to support multiple versions of the Framework on the same machine. If your system already has another version, later or earlier, of Microsoft's .NET framework installed, the 4 version will install in parallel and not affect the current installation(s).

EPIC uses an SQL database and as part of the installation, Microsoft's free database server, SQL Server 2008 Express Edition, can be installed. However if your organisation already has a Microsoft SQL Server installation, then the database can be hosted on that system if preferred.

2.2 Hardware

2.2.1 Machines

EPIC is designed around a client/server architecture and multiple machines will typically be used in a standard configuration.

The most important machine in the configuration is the machine allocated the EPIC server role. This machine will be at the heart of the configuration and will perform the majority of the data processing for the system.

Recommended server specification:

- 3 GHz Pentium 4 (or equivalent)
- 1 GB RAM (2 GB for Windows Vista)

- 100 MB of free disk space (although more will be required for file storage or if installing SQL Server)

Optional additions:

- RAIDed hard disks
- Redundant CPUs and power supplies
- UPS

Although the clients and server can be installed on one machine, typically, satellite machines will have clients installed that connect to the EPIC server.

Recommended client specification:

- 2 GHz Pentium 4 (or equivalent)
- 512 MB RAM (1 GB for Windows Vista)
- 30 MB of free disk space

2.3 Communication Requirements

If you are going to use EPIC for communications, you will need a means of electronic communication with the outside world. The communication methods you choose to support will either be an internal decision agreed by your organisation, or imposed on you by an external company with which you want to exchange data.

Both your organisation and the company with which you wish to exchange files need to agree on a common connection method by which to exchange data (unless you are exchanging data via a Value Added Network), otherwise it will not be possible to establish a connection.

The matrix below summarises the communication protocols supported by the different network protocols in EPIC. A summary of the supported communication protocols can be found in Appendix A and a more detailed description can be found in VM-0001-10 Communications Protocols Reference.

	TCP/IP	ISDN	X.25
OFTP 1 & 2	✓	✓	✓
AS2	✓		
FTP	✓		
SFTP	✓		
X.400	✓		

2.3.1 TCP/IP Support

TCP and IP were developed by America's Department of Defence (DOD) as a research project to connect a number of different networks designed by different

vendors into a network of networks. It was initially successful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) and is now a fundamental part of the largest network of computers in the world, the Internet.

Most companies have some form of permanent connection to the Internet, either via a leased line or broadband connection. EPIC can utilise this connection to make and receive TCP/IP connections, without the need for any additional hardware.

2.3.2 ISDN Support

Integrated Services Digital Network is a telephone system network. Prior to the ISDN, the phone system was viewed as a way to transport voice, with some special services available for data. The key feature of the ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

Two types of ISDN lines are commonly available:

- Basic Rate (BRI)
- Primary Rate (PRI)

A PRI ISDN circuit has up to 30 data channels, where a BRI is limited to 2.

In addition to the ISDN line, EPIC requires ISDN hardware to connect to the ISDN line.

EPIC supports two types of ISDN devices:

- ISDN card
- ISDN router

The ISDN card would be physically installed into the machine hosting the EPIC server, whilst the ISDN router would be installed on your corporate network and EPIC would connect to the route using TCP/IP.

2.3.2.1 Supported Hardware

EPIC uses the CAPI 2.0 (Common-ISDN-API) interface to access ISDN equipment connected to an ISDN line. By adhering to the standards, EPIC can make use of well defined mechanisms for communications over ISDN lines, whilst remaining independent of specific ISDN hardware manufacturers.

Within the context of OFTP, ISDN connections are commonly referred to as OFTP over ISDN; however, this is technically incorrect, as it is actually OFTP over X.25 over ISDN. Market demand for X.25 over ISDN support is relatively low and so not every ISDN hardware manufacturer supports this feature set. Consequently care must be taken when purchasing ISDN hardware.

The following manufacturers produce ISDN cards and ISDN routers that are CAPI 2.0 compliant, support X.25 over ISDN and have been tested with EPIC:

- DiaLogic
- Funkwerk AG
- Cisco

2.3.3 X.25 Support

X.25 is an International Telecommunication Union-Telecommunication Standardisation Sector (ITU-T) protocol standard and is typically used in the packet-switched networks of common carriers, such as the telephone companies.

EPIC provides X.25 support using XOT, which is an abbreviation for X.25 Over TCP. This allows X.25 packets to be sent over a Transmission Control Protocol/Internet Protocol (TCP/IP) network instead of an X.25 network.

EPIC communicates with an XOT-capable router using XOT over a TCP/IP network and the router makes the actual X.25 connection.

To support X.25 EPIC requires the following:

- An X.25 line
- An XOT capable router

2.3.3.1 Supported Hardware

EPIC requires an XOT capable router to support XOT connections. The entry level Cisco model that supports XOT is the Cisco 805, with ISO 12.2 and the IP Plus feature set. However, other routers in the Cisco range have been tested and are also supported.

3 EPIC Database

EPIC operates using a Microsoft SQL database, which can be hosted on either:

- Microsoft SQL Server 2008 Express Edition (free from Microsoft)
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005
- Microsoft SQL Server 2000

Supplied as part of the EPIC installation media is a copy of Microsoft's free database engine, SQL Server 2008 Express Edition. For the majority of installations the Express Edition of SQL Server is more than sufficient; however, if your organisation already has a copy of the full edition of Microsoft SQL Server 2000, Microsoft SQL Server 2005 or Microsoft SQL Server 2008, then the database can be created and hosted by either of these database engines.

3.1 Hosting the Database

The database engine, either the Express Edition or the full SQL server, can be installed on the EPIC server machine or on a separate machine within the corporate network. EPIC can then be configured to connect to either a local or remote database engine.

Hosting the database engine on the local EPIC server machine ensures that even in the event of a corporate network failure, EPIC will remain operational; however, hosting the database on a centralised database server could be more practical from a backup perspective.

3.2 Installing the Database

Installing Microsoft SQL Server 2008 Express Edition is optional, but by default will be installed as part of the standard EPIC installation.

If the EPIC database is going to be hosted on a Microsoft SQL Server 2000, Microsoft SQL Server 2005 or Microsoft SQL Server 2008, you do not need to install Microsoft SQL Server 2008 Express Edition. However, the Microsoft SQL server 2000, 2005 or 2008 will need to be installed and operational before the EPIC database can be created and the EPIC server started for the first time.

3.3 Creating the EPIC Database

When the EPIC server is started for the first time (following an installation using the 'Custom' option), a list of available SQL servers is presented to the user. From this list the appropriate EPIC database server can be selected.

If the database is not being hosted on the Microsoft SQL Server 2008 Express Edition installed as part of the EPIC installation, then a username and password with appropriate access permissions on the alternative SQL server database

engine will be required. These details will be provided by your network database administrator.

3.4 Database Backup

If the EPIC database has not been created on a centralised database server, then some consideration will need to be given as to how the database and associated data files are going to be backed up.

Installed as part of the EPIC installation is a database backup utility, which can be used to take a snapshot of the current database configuration and associated file details.

NOTE: This utility does not backup the data files held on the local hard disk and these would need to be backed up separately.

The backup utility requires someone to run the application manually and choose where the database backup should be placed; however, Microsoft SQL Server is common in corporate network environments and most backup solutions e.g. Veritas BackupExec, have SQL server backup agents that can be used to automate the database backup as part of your corporate backup strategy.

4 EPIC Clients and Server

4.1 Distributed Clients

EPIC has been designed to operate in a multi user, client/server architecture, which means that if a PC can connect to the corporate network hosting the EPIC server, either via the LAN, WAN, VPN or World Wide Web, users can use the EPIC clients and connect to the central server.

All the users will see the same centralised information and be able to work with EPIC at the same time.

4.2 Introduction

In this section we will describe the EPIC applications, what their function is and who will be using them.

The EPIC applications, listed below with their shortcut icons, are:

EPIC Administrator 

Postbag Workstation 

Administrator's Workstation 

Communications Monitor 

ENGDAT Workstation 

EPIC Monitor 

Batch Administrator 

4.3 EPIC Server

The EPIC server is the heart of EPIC. It co-ordinates EPIC's operations and is aware of any other servers in the EPIC installation.

4.3.1 Who would use the EPIC Server?

The server is hosted on a centralised machine, which would typically only be accessible to personnel responsible for key applications e.g. IT managers, network infrastructure staff, server application support staff.

4.4 EPIC Administrator

The EPIC Administrator is the administrative control centre of EPIC. Before you can begin to use EPIC to process your files, you must use the EPIC Administrator to set up all your details, including information about your company, your trading partners, and your communication details. The EPIC Administrator is also used to set up the EPIC application to suit your system requirements.

Once the configuration of the Administrator has been completed, there are typically few modifications or alterations that need to be made on a day-to-day basis.

The usage of the EPIC Administrator is beyond the scope of this publication. A brief overview is given below; however, for full details on how to use this application to configure your system, please refer to the separate Administrator's Guide.

4.4.1 Who would use the EPIC Administrator?

The Administrator would typically be used by a network administrator or an IT manager, who would be responsible for the setup and configuration of the system.

4.5 EPIC Postbag Workstation

The Postbag Workstation application is one of the main day-to-day usage applications of EPIC.

It allows you to track the files in each postbag within the system, linking the communications details of files sent and received, together with any workflow processing that has taken place on a per file basis.

4.5.1 Who would use the Postbag Workstation?

The Postbag Workstation would be used by someone who wishes to track inbound and outbound files in EPIC. This would typically be someone whose role is to monitor the operation of EPIC.

4.6 EPIC Administrators Workstation

The Administrators Workstation application can be used to further analyse the processes involved when using workflows.

Initially, unless restrictions have been made under EPIC security, you can see a list of inbound and outbound workflow files, files that have been received, sent or scheduled via EPIC comms, as well as error files and archived files.

You can also manually schedule files and extract files from the system, make calls and view the communications log while a call is being made.

4.6.1 Who would use the EPIC Workstation?

The EPIC Administrators Workstation offers a lower level of file auditing compared with the Postbag Workstation; however, the same subset of users would typically use the EPIC and Postbag Workstation.

4.7 EPIC Communications Monitor

The communications monitor allows users to view statistics and live information about communications sessions in EPIC. This client application is purely a monitor and therefore has very little functionality. Other clients are available for the functional aspects of EPIC.

4.7.1 Who would use the EPIC Communication Monitor?

The EPIC Communication Monitor can be used to diagnose connection issues, as well as monitor day-to-day connections. Consequently, the communication monitor would be used by the day-to-day operators of EPIC and communication and network infrastructure department.

4.8 EPIC Batch Administrator

The EPIC Batch Interface allows you to automate tasks such as setting up new Comms entries, scheduling files for immediate sending and many other tasks.

If you have a sequence of operations to be performed regularly, or if you want EPIC to be run by non-computer personnel, you may automate it by setting it to run in batch mode.

The Batch Administrator allows you to configure the settings for running EPIC in batch mode.

4.8.1 Who would use the EPIC Batch Administrator?

The EPIC Batch Administrator would only need to be installed on a machine that needs to send batch commands to EPIC. Typically this would be a system running an internal application, which needs to control EPIC. This client would not typically be required on an individual's PC workstation.

5 EPIC Satellite Servers

A computer cluster is generally thought of as a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks.

EPIC extends the cluster concept to an application level, where individual tasks performed by EPIC can be distributed to satellite servers throughout the local area network, whilst still appearing as a single application.

EPIC monitors satellite servers to ensure they are operational, and in the event of a failure the master server decides what appropriate action should be taken e.g. keep trying to connect, start another instance of the task on a separate server etc.

5.1 Benefits of Satellite Servers

5.1.1 Availability

Satellite Servers provide system robustness that reduces or eliminates planned and unplanned downtime and ensures high performance with backup and failover functionality. If one component in the system fails, another component in the EPIC installation replaces it with minimal or no noticeable difference to users.

5.1.2 Maintenance

Satellite Servers simplify administrative maintenance because multiple servers are managed as a single system. Not only does this minimise required maintenance efforts, it also ensures that servers can be added or removed from the EPIC installation without requiring reconfiguration and downtime.

Additionally, the workload can be shifted onto other satellite servers while the maintenance or upgrade is performed on the unloaded server.

5.1.3 Scalability

The number of satellite servers or configuration can easily be expanded to accommodate changing conditions and requirements of the organisation. New components can easily be added as system load increases.

5.1.4 Load Balancing

Consumption load can be distributed evenly among multiple instances of satellite servers within the installation to ensure that no single device is overwhelmed. If one server starts to get overloaded, requests are forwarded to another server with available capacity.

Load balancing schemes are especially important for installations where it is difficult to predict the number of requests that will be issued to a server.

5.1.5 Distributed Environment

The EPIC installation can be configured to run in a decentralised, distributed environment. The modular design allows organisations to split tasks across multiple servers to maximise system resources throughout the installation.

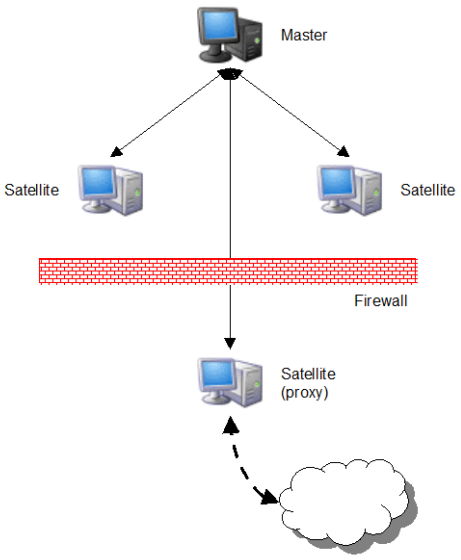
5.2 Satellite Server Framework

EPIC is a multi-user client-server communications and business integration platform that scales for use in small, medium and high workload environments. The EPIC framework supports the installation of multiple EPIC servers in a networked environment to enable distributed communications and workflow processing.

Key features of the EPIC framework are:

- An installation of servers, consisting of a single master server responsible for directing work to a number of satellites.
- Servers in the installation connected using TCP/IP with built-in health checking of the connection and retries if the connection is lost.
- The ability to run discrete aspects of the server processing as tasks on satellite servers.
- A mechanism for directing work requests from a task on one satellite server to another, via the master.
- A communications proxy task that may be used to isolate server tasks running on satellites from external communications networks.
- An operator console on the master server that allows satellite servers and tasks to be started or stopped from time to time, and work to be redistributed among satellites.

The diagram indicates the relationships between master and satellite servers:



The number and configuration of satellite servers in any given EPIC deployment may be altered to suit your individual requirements. Satellite servers can be easily added to the installation (and removed from it) using commands provided in the master server's console.

5.3 EPIC Worker Tasks

EPIC is divided into a number of worker tasks; each can either be run from the master EPIC server or configured to run from a satellite server.

Below is a list of some of the key EPIC tasks; however, a complete list of tasks is available in the Administrator Guide, VM-0001-04.

- Communications Task

Establishes outgoing, and handles incoming, communication sessions for various protocols.

- Communications Manager

Coordinates communications tasks running on different servers.

- Communications database and file manager

Manages database and file system access for the communications task.

- Communications proxy

Isolates the communications task from the real external network by acting as intermediary for incoming and outgoing data.

5.4 Configuration

Care must be taken when considering which tasks should be implemented on which servers. Although it is theoretically possible to have a satellite server for every task, this would be costly from a hardware perspective and probably be excessive.

5.4.1 Typically Configuration

Typically a EPIC system is split into three servers and the optional proxy server:

- The master server
- The workflow server
- The communication server
- The proxy server (optional)

The master server hosts the following tasks:

Communications Manager	Client connection manager	Housekeeper
Communication	Event manager	Workflow Processor

database and file manager		
Directory monitor	Event action processor	Select workflow

The workflow server hosts the following tasks:

File analyser	File splitter	EDIFACT security
File manager	Scheduler	DFS file processor
Code page conversion	Xe mapper	Alter file
XLATE processor	Write to file	Postbag dump
Write to Windows log	WebSphere MQ	Data security
Wait for comms	ENGDAT	SAP job
Submit to Darwin	Send e-mail	SAP update
Run application	Print report	

The Communication Server hosts the following task:

Communications Task		

The proxy server hosts the following task:

Communications proxy		

In this typical configuration, the master server would be configured to move any tasks that are not responding between the workflow and the communication server. This configuration ensures that the workflow and communication aspects of EPIC remain predominantly separate, unless a problem occurs, whilst still retaining a level of redundancy in the configuration.

5.4.2 High Communication Load

This configuration is almost identical to that of the typical configuration; however, additional communication satellite servers are introduced into the installation.

This configuration assumes that although the communication workload has increased, the system resources required to process the inbound/outbound i.e. the workflow workload, has remained relatively static.

In the event of a failure in one of the communication servers, the master server could be configured to either:

- Redirect communications to the remaining communication server and continue monitoring the failed communication satellite. When the failed communication satellite server recovers, the master server will revert back to the de facto setup, and balance the connections between the two communication servers.

- The master server starts another communication task on the workflow server and balances the communication traffic between the remaining communication server and the new communication task on the workflow server.

5.4.3 High Processing Load

In this scenario the inbound and outbound files require a number of translations to be carried out, reports to be generated and the results to be printed. Again we would use the typical model as a basis; however, an additional ‘mapper’ satellite server would be used to run the XE mapper, XLATE mapper and print report jobs. This would free resources on the workflow server for the remaining tasks.

In the event of a failure in the additional mapper server, the master server could be configured to either:

- Start the mapper and print task on the workflow server
- Start the mapper and print tasks on both the workflow and communication server, to distribute the workload over two machines.

6 EPIC Proxy

A proxy is a server (a computer system or an application program) which services the requests of its clients by forwarding requests to other servers. A client connects to the proxy, requesting some service, such as a connection; the proxy then provides the resource by connecting to the specified server and establishes the connection on behalf of the client.

A proxy that passes all requests and replies unmodified can be referred to as a gateway or sometimes tunnelling proxy.

The EPIC proxy acts as both a forward and reverse proxy: forward, in the sense that it makes calls out to external users, and reverse, in that it accepts incoming calls from external users.

6.1 Benefits of a Proxy

The proxy acts as a broker between the external trading partner and the internal EPIC server. Consequently, external trading partners never connect directly to the EPIC server, but always go via the proxy.

The proxy is used to determine which of EPIC's communication tasks should handle the inbound connection. On receipt of an inbound connection, the proxy initiates a connection to EPIC's Communication Manager task to determine which satellite server to direct the inbound connection to. This level of awareness allows the proxy to redirect an inbound connection to an alternative server if the Communication Manager task determines it is required.

6.2 Typical Configuration

The proxy can be placed on the EPIC master server local computer or at specific key points between the user and the destination server. However, the proxy is typically installed in the demilitarised zone (DMZ), between the corporate firewall and the external trading partner.

The EPIC proxy is configured to listen for inbound connections from external trading partners on a number of ports. Typically, ports include:

- 3305 OFTP 1 traffic
- 6619 OFTP 2 traffic
- 21 FTP traffic
- 22 SFTP traffic

6.2.1 Inbound Calls

When it receives an incoming call from an external client, the proxy makes an outgoing call to the EPIC communications server and exchanges data between the client and communications server. The proxy configuration defines to which

communications server port an incoming call on any given proxy port is forwarded.

6.2.2 Outbound Calls

When the EPIC communications server needs to call out to an external user, the communications server configuration indicates that it should call the EPIC proxy, by default on port 2999, and pass to it the user's call details. When the EPIC proxy receives an incoming call from the communications server, it accepts the user's call details and makes an outgoing call to the external user and exchanges data between the communications server and the external user.

7 Security

7.1 Client Connection Security

Although many people believe their corporate network is secure, there is always the possibility of someone eavesdropping on data being exchanged between two PCs. Consequently, it is important to secure the transmission of information, even if it is only being sent over the corporate network.

By default, the EPIC clients connect to the master server using TCP/IP port 3547; however, the data sent over this connection is un-encrypted.

To secure the connection, the clients can be configured to connect to the master server on port 3548, which secures the connection by using SSL technologies.

The SSL connection is transparent to the EPIC end user. However, the underlying connection is now secure and any data exchanged between the EPIC client and master server is encrypted. Therefore, even if it was intercepted by an unscrupulous third party, they would not be able to decipher the data being exchanged.

7.2 User Security

User security is built into the system, but has to be selected explicitly if you want to use it.

User security is a feature of EPIC which, if used as intended, guarantees the security of the system within your company. Although you do not have to enforce any security measures, it is advisable, at the very least, to prevent unauthorised users from gaining access to any part of EPIC.

User security serves two purposes:

- To stop unauthorised users from accessing the system
- To restrict authorised users' permissions within the system

User security is turned on or off at a global level (i.e. it affects all the applications). When turned on, it can be set to one of two modes:

- Use EPIC's own security
- Use Windows Active Directory security

7.2.1 EPIC's own security

For full security to be maintained, someone at your company must be designated to manage the security settings from within the EPIC Administrator. For this purpose, we have pre-configured a System Administrator for you. This user has been set up with full edit permission for the EPIC Administrator.

Using EPIC security, when an application connects to the server the user will be asked for a username and password (though passwords may be blank if the Use passwords option has not been selected). The username and password are then validated to see if the user is authorised to log on.

7.2.2 Windows Active Directory security

Using Windows Active Directory security, EPIC can import users and groups from the Windows Active Directory. Users will have to be logged on to Windows with a valid account in order to access any features of EPIC. Imported users can be used in all the same ways as EPIC users to access other user-based functionality.

Even when using Windows Active Directory security, a designated System Administrator must still be present in the EPIC security configuration. He will be able to log on to the EPIC Administrator and set user permissions for each Windows user group. He will also have full access to all the EPIC clients.

7.3 Users, User Groups and Permissions

EPIC is a multi-user application that enables various people within a company to handle various aspects of file processing within that company.

However, not everybody will want to see the same data. For example, the IT Manager, who needs to administer the EPIC system, will only need to see the Administrator application, whereas those people concerned with the actual sending and receipt of files will only be interested in the Workstation application.

7.3.1.1 Users

Defining users in the system allows each person who uses EPIC to be identified. Anyone not recognised by EPIC security is denied access to the system.

7.3.1.2 User Permissions

User permissions can be used for two purposes:

- for security, to restrict users to specific areas
- for simplicity, to show users only what they need to see

User permissions define the areas of EPIC to which the user may have access, and the functions that he can carry out within those areas. A user permission might be, for example, permission to use the EPIC Administrator and being given View access to a specific view (page) of an application; with View access, he will be able to read the data, but will not be able to edit it.

Every user can have his own set of permissions that dictate what he can or cannot do within the system.

There are basically two levels of user permissions – granting access to one or more specific applications, and granting access to specific areas within those applications.

7.3.1.3 User Groups

A user group is a convenient way to allow a number of users to share the same permissions. A user group has a set of permissions associated with it. Any users who are assigned to that group are automatically given those permissions.

You can define users without assigning them to a group. Then you would assign individual permissions to them.

Users can be assigned to any number of groups, and are automatically given the permissions from all the groups they have been assigned to.

If Windows Active Directory Security is being used, then the user groups defined in Windows Active Directory will be used. EPIC allows users to assign a set of EPIC permissions to a Windows Active Directory user group. In this scenario, the relationship between users and user groups has to be managed from within the Windows environment, not from within EPIC.

7.3.1.4 Communities

A community is a way to restrict the data that users and groups can view in the EPIC applications. A user or group can be a member of one or more communities.

In the administrator client, when a user logs on who is a member of one or more communities, that user can then only view networks and trading partners that are associated with the communities that they are members of.

In the workstation client, when a user logs on who is a member of one or more communities, they will only see files that are associated with networks that they have permission to view.

In the communications monitor client, only sessions between networks that the user has permission to view are visible in the session list.

8 Systems Integration

Streamlining the communications between your company and your trading partners is only half the story. To streamline the whole end-to-end process, EPIC will need to exchange data seamlessly with your internal systems.

EPIC integrates with in-house packages in many different ways including:

- Import and export directories on the corporate network
- FTP upload/download
- IBM WebSphereMQ
- Specialised SAP integration component

EPIC utilises Data Interchange's message translator, XLATE Evolution, which provides mapping functionality to translate between different internal or external message formats.

8.1 Data Flow

EPIC can integrate with internal systems in a number of different ways:

- Import/export directories
- FTP upload/download
- IBM WebSphereMQ (requires IBM WebSphereMQ client V5.3 or greater to be installed on the EPIC server, Advanced MQ requires IBM WebSphereMQ client V7.0 or greater and IBM Message Service Client for .NET)
- SAP Interface (startRFC and tRFC)

The configuration of your current network infrastructure, corporate policies and the capabilities of your internal system will influence which integration options are applicable to you.

8.1.1 Considerations

The following questions will need to be reviewed when considering integration options between EPIC and your internal system:

❑ What common integration interfaces are available between EPIC and the internal system?

If you are using the directory or FTP integration option:

❑ What directory structure will be required?

❑ Will a single import and export directory be sufficient?

❑ Will the import and export directory need to be sub-divided by trading partner and/or message types?

❑ Will specific file names be required?

- ❑ Can the internal system import from and export to different directories?

If you are using IBM WebSphereMQ:

- ❑ Have appropriate inbound and outbound queues and channels been created?
- ❑ Will different channels be required for different trading partners and/or message types?

If you are using the SAP interface:

- ❑ Is the startRFC or tRFC most suitable?

8.2 File Formats

Throughout the world there are numerous standards, each with their own syntaxes, file formats and array of messages. Some standards are more commonly used within a single market sector, whilst others have been adopted by multiple sectors. Some are developed by committees and influential bodies within a given sector, whilst others are bespoke to a single company.

The array of standards and associated messages can be bewildering; however, to complicate matters further, the file formats used by your internal system are nearly always different to the formats your trading partners will be using.

To ensure that you can easily integrate the data you are exchanging with your trading partners, EPIC has a powerful any-to-any mapper called Xe (XLATE Evolution), which seamlessly integrates with EPIC and will automatically convert between internal and external file formats.

XLATE Evolution supports the following syntaxes:

ANSI X12	VDA
EANCOM	XML
EDIFACT	ebXML
EDIFACT V4	SAP IDoc
ODETTE	CSV
TRADACOMS	UCS

Maps are developed outside of EPIC in XLATE Evolution's development application. Once a map has been developed and tested, it can easily be deployed in EPIC.

8.2.1 Considerations

When reviewing the file format integration options, the following questions will need to be answered:

- ❑ What format does my internal system import?
- ❑ Is a specification for the import file format available?
- ❑ What data is required for the internal import file format?
- ❑ Is the required data available in the inbound message?
- ❑ What file format does your internal system export?
- ❑ Is a specification for the export file format available?
- ❑ Is the export specification different for different message types e.g. despatches advices messages and invoice messages?
- ❑ What data is required for the external file format?
- ❑ Is all of the required data available in the file exported from the internal system?

9 Workflow requirements

As an end user, you may be using EPIC to receive files from a trading partner. You may therefore wish to perform workflow jobs specific to the originating trading partner and workflow jobs specific to the recipient internal company.

In addition, you may be using EPIC to send files to a trading partner. You may therefore wish to perform workflow jobs specific to the originating internal company and workflow jobs specific to the recipient trading partner.

You therefore need to create at least one workflow for each of the following:

- for your Internal Company: one workflow for incoming files (the Recipient Workflow)
- for your Internal Company: one workflow for outgoing files (the Originator Workflow)
- for your Trading Partners: one workflow for incoming files (the Originator Workflow)
- for your Trading Partners: one workflow for outgoing files (the Recipient Workflow)
- an error workflow

Before you create any workflows, you need to do some preliminary analysis. Thorough analysis of your requirements at the planning stage will enable you to configure your workflows in the most practical way.

9.1 Analysis

There are a number of questions that need to be considered, to enable you to determine how many workflows you might need, and what processing they are going to perform.

You should bear in mind that each file that enters the EPIC system will start off in one postbag and end up in another. When considering the processing that your files require, consider which processes should be performed by the Originator Workflow and which by the Recipient Workflow.

You could, in theory, create a different workflow for every postbag/file-type combination, but in practice this is unlikely to be necessary, as many of your file types can probably be processed in the same way, and your trading partners may well have similar requirements.

Your objective, therefore, is to be able to set up a minimal number of workflows that will handle the required processing for all files in your system postbags.

9.1.1 Considerations

The following list of questions may help you collect the information you need. In this list, the term “file types” refers to file purpose, such as orders, forecasts, despatches, invoices, and many others.

- ❑ How many trading partners do you have, and who are they?
- ❑ What file types do you exchange with each trading partner?
- ❑ What kind of processing needs to be performed on each of the incoming file types?
- ❑ What kind of processing needs to be performed on each of the outgoing file types?
- ❑ Can files of the same type from different trading partners be processed in the same way?
- ❑ Can files of different types from the same trading partner be processed in the same way?
- ❑ In what different ways may files arrive in your system e.g. via a communications session, from a monitored directory etc)?
- ❑ What do you want EPIC to do with each file that arrives in the system, according to their file type and content, their origin and their destination?
- ❑ Do you need to translate incoming EDI files into an in-house format?
- ❑ Do you need to translate outgoing in-house files into an EDI format?
- ❑ Do you need to process any files using an in-house application?
- ❑ Do you want to take a copy of any files?
- ❑ Do you need to perform special processing on outgoing files before or after placing them in the recipient’s postbag?
- ❑ Do you need to perform special processing on incoming files before or after placing them in the recipient’s postbag?
- ❑ What differentiates the files?
- ❑ What similarities do the files have?

9.2 Workflows for a corporate gateway scenario

For detailed examples of workflows handling both incoming and outgoing files in a corporate gateway scenario, please refer to Appendix D of this guide.

9.3 Workflows for a Clearing Centre scenario

The creation of workflows for a Clearing Centre is similar to the creation of workflows for a corporate gateway. Let's take as an example two trading partners who communicate with each other via the Clearing Centre.

Trading partner A sends in-house files to the clearing centre which are to be delivered to trading partner B by the clearing centre. Trading partner B needs EDI formatted files from all of its trading partners, and also wants them in EBCDIC format.

Trading partner A will translate his in-house files into an EDI format in his postbag's originator workflow. Trading partner B will convert the EDI data into EBCDIC in the recipient workflow of his postbag.

9.3.1 Example

Some of the processing must be done by the originator workflow, but the remainder can be done on the recipient workflow. On arrival of the file, the system can determine its originator from the communication session details, and will place the file in Trading Partner A's postbag.

Once in Trading Partner A's postbag, it will be processed as follows:

9.3.1.1 Originator Workflow 1

- ❑ map the incoming file from the in-house flat file format to the partner's format
- ❑ post to Recipient Postbag

Any further processing will then be performed by the Trading Partner B's recipient workflow.

9.3.1.2 Recipient Workflow 1

Once in Trading Partner B's postbag, it will be processed as follows:

- ❑ convert the file to EBCDIC format
- ❑ make Postbag File Available

9.4 Error workflows

Error handling is an important aspect of workflows. You should create at least one error handling workflow to ensure that, if any job in a workflow results in an error, the file will be handled appropriately and an alert will be sent to a designated user.

You can include any job in an error workflow, but most of them would not be appropriate. The most useful jobs for inclusion would be any of the following:

- E-mail: sends an e-mail to one or more specified addresses

- Windows Application Log: writes a message to the Windows application log
- Write to File: writes to a file the details of an event
- Write to MQ Message Queue: writes a message to a WebSphere MQ message queue

10 Trading Partner Communications Requirements

The communication methods you use to connect to your trading partners will either be the result of an internal decision made by your organisation, or imposed on you by your trading partners.

Both your organisation and the company that you wish to exchange files with need to agree on a common connection method to exchange data over (unless you are exchanging data via a Value Added Network), otherwise it will not be possible to establish a connection.

The connection method is a combination of a communication protocol (how the two parties will “talk” to each other once a connection is made), and a network protocol (the physical means by which the two parties will connect to each other).

If you use a VAN to connect to your trading partners, you will usually have more choice over which communication and network protocol to use.

This section provides details of communication considerations. A summary of these requirements can be found in Appendix A of this Guide.

10.1 Communication Protocols

EPIC supports a number of different communications protocols for sending and receiving all types of files. Communications protocols define the logical process by which communication between two computers is carried out. Communications protocols currently supported are:

- OFTP 1
- OFTP 2
- AS2
- FTP Server and Client
- SFTP Server and Client
- X.400

A summary of these communications protocols can be found in Appendix A at the end of this Guide and further information can be found in VM-0001-10 Communications Protocols Reference.

10.2 Network Protocols:

EPIC also supports a number of network protocols. Network protocols define the physical means by which the communication from one computer to another is made. Network protocols currently supported are:

- TCP/IP (Internet)
- XOT (X.25)

- ISDN (CAPI)

A summary of these network protocols can be found in Appendix B at the end of this Guide and further information can be found in VM-0001-10 Communications Protocols Reference.

10.2.1 Summary of protocols

The matrix below summarises the communication protocols supported by the different transportation protocols in EPIC. A summary of the supported communication protocols can be found in Appendix A and a more detailed description can be found in VM-0001-10 Communications Protocols Reference.

	TCP/IP	ISDN	X.25
OFTP 1 & 2	✓	✓	✓
AS2	✓		
FTP	✓		
SFTP	✓		
X.400	✓		

10.3 Connection options and parameters

Each of your trading partners will have to provide you with details of their communication and network protocols, and will want to know yours in return. The information to be exchanged will differ according to the protocols that are to be used.

10.3.1 OFTP 1

For an OFTP connection you will need to:

- exchange EDI codes (for all three levels – see below)
- exchange OFTP passwords, if use is agreed by both partners
- exchange details of the connection method you will be using

10.3.1.1 EDI Codes

The OFTP protocols have 3 levels of routing. Each of these levels may have its own code, but in many cases the codes are the same at all three levels. The code at all three levels may be referred to generally as an EDI code.

- Network Node – also referred to as the SSID Code or the Physical Node
- File Node – also referred to as the SFID Code
- Message Node – also referred to as the UNB Node

For further information on EDI codes, and how to create one if you do not already have one, please refer to Appendix C of this guide.

10.3.2 OFTP 2

Requirements for OFTP 2 connections are the same as those for OFTP 1, with the additional option that you may specify what type of security is required for the connection. Options to be considered are:

- ❑ whether to use the OFTP 2 security features at all
- ❑ whether to use session level encryption
- ❑ whether to use file encryption
- ❑ whether to use file signatures
- ❑ whether to use signed EERP acknowledgements
- ❑ whether to use session authentication
- ❑ which security certificates to use

Further information about OFTP 2 security can be found in the VM-0001-10 Communications Reference guide.

10.3.3 AS2

For an AS2 connection you will need:

- ❑ a permanent connection to the Internet

For AS2 connections you will need to exchange the following:

- ❑ AS2 identifier (AS2 Name)
- ❑ URL/Port of AS2 server
- ❑ encryption requirements
- ❑ MDN Receipt requirements
- ❑ current AS2 certificate
- ❑ any other details required by individual trading partners e.g. user IDs for access

Further information about AS2 can be found in the VM-0001-10 Communications Reference guide.

10.3.4 FTP

For an FTP connection, each partner may act as an FTP Server, an FTP Client or as both Server and Client. Your roles must be agreed with each other beforehand.

For an FTP connection you will need:

- ❑ a TCP/IP connection to the Internet

For an FTP connection, as a Server, you will need:

- ❑ a permanent connection to the Internet, with a fixed IP address
- ❑ to tell the client your IP address

For an FTP connection you will need to:

- ❑ agree with your trading partner which of you will be the FTP client and which the FTP server, or whether you will both be client and server
- ❑ agree the Port number for connection
- ❑ agree whether the FTP server is to be Active or Passive
- ❑ agree the directory structure to be used
- ❑ exchange user names and passwords

For further details about Active and Passive connections, and the FTP directory structure, please refer to the VM-0001-10 Communications Reference manual.

10.3.5 SFTP Client

An SFTP Client connection is a secure FTP client connection. Although the SFTP protocol is fundamentally different from FTP, it has the same connection requirements as an FTP connection.

10.3.6 SFTP Server

EPIC can host an SFTP server. For this you will need:

- ❑ a permanent connection to the Internet, with a fixed IP address
- ❑ a public certificate to identify the server to client
- ❑ to tell the client your IP address and SFTP port (usually 22)

To set up the SFTP server you will need to:

- ❑ agree the virtual directory structure to host on the server
- ❑ agree the algorithms that may be used to secure the SFTP sessions
- ❑ exchange user names and passwords

For further details about hosting an SFTP server, please refer to the VM-0001-10 Communications Reference manual.

10.3.7 X.400

For an X.400 connection you will need:

- ❑ an IP address and port number
- ❑ to decide on a name and password for your MTA
- ❑ to agree with your trading partner which X.400 protocol to use (1984, 1988 or 1988 (x.410))
- ❑ to decide on your TSAP code
- ❑ to exchange X.400 address details with your trading partner

Further information about X.400 can be found in the VM-0001-10 Communications Reference guide.

10.4 Connection methods

10.4.1 TCP/IP

For a TCP/IP connection you will need:

- ❑ a connection to the Internet, either via a leased line or a broadband connection

For a TCP/IP connection you will need to:

- ❑ exchange IP addresses
- ❑ exchange the Port numbers through which you can access each other's systems
- ❑ ensure that your firewall is configured to allow access in both directions through the specified Port.

10.4.2 ISDN

For an ISDN connection you will need:

- ❑ an ISDN line
- ❑ a suitable CAPI 2.0 compliant ISDN card or ISDN router

For an ISDN connection you will need to:

- ❑ exchange ISDN numbers.

10.4.3 X.25

For an X.25 connection you will need:

- ❑ an X.25 line
- ❑ an XOT capable router

For an X.25 connection you will need to:

- ❑ exchange X.25 NUAs

10.5 General

There are certain things that you need to consider and plan, no matter what communication method or connection network your trading partner will be using.

- ❑ the originator workflow for the trading partner's postbag (this is the workflow that will be run for files received from your trading partner)
- ❑ the recipient workflow for the trading partner's postbag (this is the workflow that will be run for files sent to your trading partner)

11 Appendix A – Communication Protocols

11.1 OFTP

OFTP was first defined in 1986 by ODETTE International Ltd, a membership organisation formed by the automotive industry for the automotive industry, which sets the standards for e-Business communications and engineering data exchange. OFTP is a protocol for exchanging data in an automated environment and initially designed to work over an X.25 network, but over the last two decades it has evolved to work over ISDN and TCP/IP networks.

OFTP is the most widely-used protocol inside Europe for the exchange of EDI data, in particular in the automotive sector, but is also commonly found in the retail, petrochemical, tax submissions and banking sectors, amongst others.

11.2 AS2

AS2 (Applicability Statement 2) is an RFC which was developed by the Internet Engineering Task Force (IETF) and Cyclone Commerce Corporation. The first draft of AS2 was first produced in late 1996. It then took a further decade before finally becoming an RFC standard in July 2005.

AS2 was an American initiative to produce a business protocol and was intended primarily as a way of bypassing VANs by having direct communications between trading partners over the Internet. Much of the success of AS2 has been confined to America, and specifically the retail sector.

11.3 FTP

FTP (File Transfer Protocol) was published as an RFC in April 1971 and since then adoption has grown steadily.

It is used to exchange all types of files, in all market sectors and is now a commonly used file transfer protocol throughout the world.

11.4 SFTP

SFTP (SSH File Transfer Protocol) is an Internet Draft protocol designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH). Its first draft was released in January 2001, and although it has never become an Internet Standard, it is widely implemented.

Although commonly used to securely traverse a remote file system, the protocol has no relation to FTP. SFTP is an exchange of command and data packets over a secure channel, usually SSH. These commands manipulate the remote file system, standardized on UNIX conventions, to effectively upload and download files.

11.5 X.400

Developed by the International Organisation Standards and the International Telecommunication Union, X.400 is a set of standards for the exchange and addressing electronic messages. The first X.400 recommendations were published in 1984 (*Red Book*), and a substantially revised version was published in 1988 (*Blue Book*). New features were added in 1992 (*White Book*) and subsequent updates.

Although X.400 was originally designed to run over the OSI transport layer, an adaptation was made to allow operation over TCP/IP and this has now become the most popular way to run X.400.

12 Appendix B – Network Protocols

12.1 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet, where parties within a single organisation can communicate, or an extranet, where parties may communicate with each other over an external but private network).

TCP/IP provides basic but high-demand services, such as file transfer and electronic mail (e-mail), across a very large number of client and server systems.

Several computers in a small company department can use TCP/IP (along with other protocols) on a single Local Area Network (LAN). The IP component provides routing from the department to the company network, then to regional networks, and finally to the global Internet.

TCP/IP is designed to be highly robust and automatically recover from any network node or phone line failure. In addition it employs flow control mechanisms, to allow for inadequacies of the receiving computer, and support for the detection of errors and lost data, with its ability to trigger retransmission until the correct data is correctly and completely received.

12.2 XOT (X.25)

XOT (X.25 over TCP/IP) enables X.25 packets to be sent over a TCP/IP network to an XOT-capable router, from where they are transported to the destination over an X.25 connection.

XOT allows users to connect to X.25 partners via an XOT router. In many cases, X.25 users prefer to install routers rather than have X.25 calls come directly into their communications applications, since the latter method can have security issues. Routers can be configured to block calls from unknown origins.

Where native X.25 is used, X.25 hardware, which can be costly, has to be connected to the machine on which ODEX is installed. However, where XOT is used, EPIC simply makes a TCP/IP connection to an XOT-capable router such as a Cisco, which can provide a sizeable cost saving.

Using an XOT router, EPIC can communicate with trading partners using either native X.25 or ISDN, depending on the routing rules and configuration of the router.

12.3 ISDN (CAPI)

ISDN (Integrated Services Digital Network) is a digital communications line that allows for the transmission of voice, data, video and graphics, at very high speeds, over standard communication lines.

The increasing need to transfer large volumes of EDI data, in particular CAD/CAM drawings, has focused attention upon high speed, low cost, communication.

Two types of ISDN line interface are available: Basic Rate (BRI) and Primary Rate (PRI). An ISDN line consists of two different channel types:

- B-Channel – Carries bearer services, such as digital data, video, and voice.
- D-Channel – Carries control and signalling information and can also carry packet mode data.

BRI includes two 64 kbps (kilobits per second) B-channels and one 16 kbps D channel. PRI in Europe consists of 30 B channels and one 64 kbps D channel, while in North America and Japan 23 B channels and one 64 kbps D channel are provided.

Common ISDN API (CAPI) is an application-programming interface used to access ISDN equipment. CAPI enables applications to access ISDN adapters in a straightforward manner and allows unrestricted use of their functions through a standardized software interface. This interface, which offers a single point of access to different ISDN services such as data, voice and fax, can then be used by applications.

The use of CAPI allows applications to communicate over ISDN lines without having to cater for differences in hardware manufacturers' specifications. Furthermore, in the event of future hardware developments, applications will remain unaffected, as CAPI will make any changes transparent to the application.

13 Appendix C – EDI Code Creation

You may already have an EDI code if you belong to one of the international numbering organisations, such as GS1 or Duns and Bradstreet. If you do not yet have an EDI code, you can create one as described in the next three sections. Please note that you will need to know whether you will be exchanging Odette/EDIFACT, Tradacoms or VDA messages with your trading partners. If you use more than one of these standards, you may need more than one EDI code.

13.1 The Makeup of an Odette/EDIFACT EDI Code

Network and File Node EDI codes may be up to 25 characters long but at interchange level an EDI code may be as many as 35 characters. The codes should be made up using the following list of characters and no others.

Character	Description
A to Z	Uppercase alphabetic characters
0 to 9	Numeric characters
-	Hyphen
/	Slash or Oblique
,	Comma
.	Full Stop
&	Ampersand
(	Left hand bracket
)	Right hand Bracket
	Blank or space (CAUTION - this is NOT recommended as some systems cannot cater for it).

There are currently no standards for EDI codification schemes. Obviously it is vital that the code should be unique. New EDI users have a number of choices available to them.

- Choose their company name (not recommended)
- Be allocated an EDI code by a third party network (VAN), trading partner or numbering organisation
- Derive their own EDI Code

If users wish to take the latter course of action, the following are the Odette recommendations for the structure of an EDI code.

Name	Description

Code Prefix	The letter ‘O’
ICD Code	The ICD (International Code Designator) is a 4 character code as specified by the ISO standard ISO 6523. This identifies a standards organisation responsible for managing a numbering scheme. The scheme could either be an international scheme, such as the European Article Numbering Association (EAN) or a national scheme such as the U.K. Company Registration number.
Company Code	This is the code assigned by the agency specified in the ICD code above. If it is less than 14 character positions, then it should be right aligned and zero padded to the left.
Sub Address	This alpha-numeric field is a user assigned sub-address. It can identify various Physical Addresses within an organisation.

An example EDI code for Data Interchange Plc would be :-

O09320000000020780 41SYS001

O	is the code prefix
0932	is the ICD for the U.K. company registration scheme
2078041	is the Company Registration number for Data Interchange Plc
SYS001	is a locally assigned code to describe the EDI entity

Please note that this is a recommendation for the formation of an EDI code and NOT a standard.

13.2 The Makeup of a Tradacoms EDI Code

Network and File Node EDI codes may be up to 25 characters long but at interchange level a Tradacoms EDI code must be 13 numeric characters long. In the Tradacoms standard, EDI codes are referred to as ANA codes and may be obtained from one of the standards bodies, such as DUNS or GS1.

If users prefer not to use the standards bodies, the following are the Data Interchange recommendations for the structure of a Tradacoms EDI code.

Name	Description
ICD Code	The ICD (International Code Designator) is a 4 character code as specified by the ISO standard ISO 6523. This identifies a standards organisation responsible for managing a numbering scheme. The scheme could either be an international scheme, such as the European Article Numbering Association (EAN) or a national scheme such as the U.K. Company Registration number.

Company Code	This is the code assigned by the agency specified in the ICD code above. If it is less than 9 character positions, then it should be right aligned and zero padded to the left.

An example Tradacoms EDI code for Data Interchange Plc would be :-

0932002078041

0932 is the ICD for the U.K. company registration scheme

2078041 is the Company Registration number for Data Interchange Plc.

Please note that this is a recommendation for the formation of an EDI code and NOT a standard.

13.3 VDA EDI Codes

Network and File Node EDI codes may be up to 25 characters long but at interchange level an EDI code can only be a maximum of 9 characters.

For VDA communications, users are normally allocated an EDI code by their trading partner. This EDI code is usually their supplier code. Trading partner EDI codes are usually the trading partner's customer code.

14 Appendix D – Workflow examples

This section provides examples of some typical scenarios, the workflows created to handle them, and the requirements that led to those workflows being created. The examples relate to a corporate gateway scenario.

14.1 Sending files from an Internal Company to a Trading Partner

Let's start by considering the workflows for the files that come into your EPIC system from your own internal systems, which will ultimately be sent to one of your trading partners. You will need an Originator Workflow, at the very least. You may also need one or more supplementary workflows if not all outgoing files can be processed in exactly the same way.

You need to consider the following:

- What types of files will you process e.g. invoices, orders, despatch advices, CAD/CAM files...?
- Will all files of the same type be of the same format e.g. CSV, XML, TXT, IDoc?

If all files of the same type are also of the same format and require exactly the same processing, then you would only need a single workflow for each different file type. However, for any files that require different processing because of certain of their attributes, you will need to create one or more additional workflows.

One of the requirements of the workflow system is to determine what type of file it is processing. Since EPIC can obtain very little information from a basic flat file (i.e. any file that is not an EDI file, an XML file or a SAP IDoc), it is the user's responsibility to ensure that the system can recognise non-EDI files, either from their filename or from their data source e.g. designate a specific directory to contain only files of a certain type, such as invoices.

However, for EDI files, XML files and SAP IDoc files, EPIC is able to analyse the file and determine who the originator and recipient are.

14.1.1 Originator processing in the Internal Company postbag

Let's take as an example a user who has five trading partners, to whom he sends invoices and despatch advices. His internal system creates flat files and places them in separate directories according to the file content (invoice or despatch advice). This means that, when he instructs EPIC to pick up files from those directories, he can be sure what type of files will be in each directory.

He wants to convert each flat file into an EDI file and send it to the appropriate trading partner. For one of his trading partners, he needs to convert the file into EBCDIC format before sending it to them.

14.1.1.1 Originator or Recipient Workflow?

Some of this processing must be done by the originator workflow, but the remainder can be done on the recipient workflow. On arrival in the Internal Company postbag, the system can determine neither the target recipient of the file nor the type of file, as it is a basic flat file. Therefore the first job of the originator workflow is to match the file to a new workflow, using workflow selectors based on the data source, and exit the current workflow.

The new workflow will process only files from the appropriate data source – either invoices or despatch advices. It will map the files into an EDI format. Once in an EDI format, the system can determine the target recipient and post the file to the appropriate recipient postbag. This scenario is described below.

14.1.1.2 Multiple Originator Workflows

Workflow 1

- Match the file to a workflow using workflow selectors based on the data source

The Match Workflow job will match each file to a new workflow, based on its data source (either the monitored directory for invoices or the one for despatch advices) and exit the current workflow. The new workflow will then continue the processing.

Workflow 2

This is the workflow for invoices.

- Map an invoice file from flat file format to EDI format
- Post to Recipient Postbag

Any further processing will then be performed by the Trading Partner's recipient workflow.

Workflow 3

This is the workflow for despatch advices.

- Map a despatch advice file from flat file format to EDI format
- Post to Recipient Postbag

Any further processing will then be performed by the Trading Partner's recipient workflow.

14.1.2 Recipient processing in the Trading Partner postbag

Once a file has been processed by the Internal Company Originator Workflow, and any supplementary workflows, it should be posted to the postbag of the appropriate trading partner, where it will be processed by the trading partner's Recipient Workflow.

Ideally the user should create a workflow which can be used for as many of his trading partners as possible. For any non-standard processing, he can create separate or additional workflows.

Using the same example as above, once in the Recipient's Postbag, he will require a workflow which will do the following:

- Convert the file encoding from ASCII to EBCDIC (applicable to one trading partner only)
- Make the file available to the trading partner (applicable to all his trading partners)

To achieve this processing for all five of his trading partners' files, this user will need just two different workflows:

Workflow 1 (applicable to one partner only)

- Convert File Encoding
- Make Postbag File Available

Workflow 2 (applicable to all other partners)

- Make Postbag File Available

14.2 Receiving files from a Trading Partner into an Internal Company

Now we need to consider the workflows for the files that come into your EPIC system from your trading partners, which will ultimately be routed to one of your internal departments or to your internal systems. You will need an Originator Workflow for each trading partner, but in many cases it may be possible to use the same workflow for several trading partners. You may also need one or more supplementary workflows if not all incoming files from each trading partner can be processed in exactly the same way.

You need to consider the following:

- ❑ What types of files will you receive e.g. invoices, orders, despatch advices, CAD/CAM files...?
- ❑ Will all files of the same type be of the same format e.g. EDI?

As for the originator workflow of the Internal Company, if all files of the same type are also of the same format and require exactly the same processing, then

you might only need a single workflow for each different file type. However, for any files that require different processing because of certain of their attributes, you will need to create one or more additional workflows.

You should try to create a workflow which can be used by as many of your trading partners' postbags as possible. For any non-standard processing, you can create separate workflows. It is to be expected that most of your incoming files will be in some kind of standard format, such as EDI, XML or IDoc, and that most will need to be translated into an in-house format so that your internal systems can use them.

14.2.1 Originator processing in a Trading Partner postbag

Let's take as an example a user who has three trading partners, two of which send him orders in a standard EDI format, and one who sends him orders in IDoc format. He wants to translate each incoming order file into an in-house flat file format, and then pass the file to his own ERP system.

14.2.1.1 Originator or recipient workflow?

Some of the processing must be done by the originator workflow, but the remainder can be done on the recipient workflow. On arrival in the Trading Partner's postbag, the system can determine the originator of the file and the type of file (since it is dealing with a structured file, not a flat file). Therefore the first job of the originator workflow is to analyse the file to determine the originator and file type.

Next, he wants to translate the file into a format that his ERP system can use, post the translated file to the recipient's postbag (i.e. the postbag of his Internal Company), make the file available to his ERP system and automatically send an e-mail alert to the Resource Planning department.

This scenario is described below.

14.2.1.2 Single Originator Workflow

Workflow 1

- Analyse the data content of the file to determine enveloping information (originator, recipient, document type, etc)
- Map the incoming file from the partner's format to in-house flat file format
- Post to Recipient Postbag

Any further processing will then be performed by the Internal Company's recipient workflow.

14.2.2 Recipient processing in the Internal Company postbag

Once a file has been processed by the Trading Partner's Originator Workflow, it should be posted to the postbag of the appropriate Internal Company, where it will be processed by the Internal Company's Recipient Workflow.

In our current example, the user wants to pass each incoming order file to his ERP system and send an email to the Resource Planning department to let them know of its arrival. To achieve this processing for all his order files, this user will need just one workflow:

Using the same example as above, once in the Recipient's Postbag he will require a workflow which will do the following:

- Place each incoming file in a directory from which his ERP system can pick it up
- Send an e-mail to the Resource Planning department

This can be achieved by the workflow below.

14.2.2.1 Single workflow for all files

Workflow 1 (to process all incoming orders)

- Make Postbag File Available – marks a file as "Released" or "Held" and makes the file visible to authorised users.
- Export – copies a file to a specified directory and marks it as Taken
- E-mail – sends an e-mail to one or more specified addresses