ARCHITECTURE GUIDELINES

For Trans-European Telematics Networks for Administrations

Annexes

Version 6.1

European Commission
Enterprise DG
200, Rue de la Loi
B-1049 Brussels

E-mail : entr-ida@cec.eu.int
www.europa.eu.int/ispo/ida

European Commission
Enterprise DG
Interchange of Data between Administrations Programme

***Author**: Enterprise DG*
Brussels, June 2002

Contents

1 INTRODUCTION 5

1.1 DOCUMENT STRUCTURE 5
1.2 REFERENCES 5
1.3 PROPRIETARY PRODUCTS 5

2 SERVICE PROFILES 6

2.1 CHARACTER SETS 6
2.2 DOCUMENT ARCHIVING SERVICES 6
2.2.1 File Compression Techniques 6
2.3 DOCUMENT EXCHANGE SERVICES 7
2.3.1 PDF (Portable Document Format) 8
2.3.2 SGML (Standard Generalised Mark-up Language) 8
2.3.3 DSSSL (Document Style Semantics and Specification Language) 8
2.3.4 HTML (Hypertext Mark-up Language) 9
2.3.5 XML (eXtensible Mark-up Language) 9
2.3.6 XMI (XML Metadata Interchange) 10
2.3.7 UML (Unified Modelling Language) 10
2.3.8 WebDAV 11
2.3.9 GIF (Graphics Interchange Format) 11
2.3.10 TIFF (Tag Image File Format) 11
2.3.11 JPEG (Joint Photographic Experts Group) 12
2.3.12 CGM (Computer Graphics Metafile) 12
2.4 CONTENT INTEROPERABILITY SERVICES 13
2.4.1 XML-Based Standards 13
2.4.2 EDI Services 14
2.5 WORLD WIDE WEB (WWW) SERVICES 15
2.5.1 Basic WWW Functionality 15
2.5.2 DOM (Document Object Model) 15
2.5.3 CSS (Cascading Style Sheets) 16
2.5.4 XUL (Document Object Model) 16
2.5.5 WAI (Web Accessibility Initiative) 17
2.5.6 WCAG (Web Content Accessibility Guidelines) 17
2.6 MIDDLEWARE AND INTERNAL INTERFACES 18
2.6.1 Remote Procedure Call 19
2.6.2 CGI (Common Gateway Interface) 19
2.6.3 CORBA 20
2.6.4 Distributed Application Architecture 21
2.6.5 Internal Interfaces 25
2.7 MESSAGE TRANSFER SERVICES 26
2.7.1 X.400 26
2.7.2 SMTP 27
2.7.3 Message Store Services 28
2.7.4 MIME 28
2.8 FILE TRANSFER SERVICES 29
2.8.1 FTP and HTTP protocol 29
2.9 WORKFLOW MANAGEMENT 30
2.9.1 Workflow Management Coalition 30
2.10 DIRECTORY SERVICES 31
2.10.1 X.500 32
2.10.2 LDAP 33
2.11 NETWORK MANAGEMENT SERVICES 34
2.11.1 SNMP 34
2.11.2 Directory-Based Management Services 35
2.12 GROUP WORKING 37
2.13 CARRIER TELECOMMUNICATION SERVICES 38
2.13.1 Circuit Switched Services, ISDN 38
2.13.2 LAN-LAN Interconnection Services 39
2.14 WAN SERVICES 40
2.14.1 IP Version 4 (IpV4) 40

2.15 SECURITY SERVICES AND SECURE CONNECTIONS 42
2.15.1 VPN (Virtual Private Network Services............ 42
2.15.2 PKI (Public Key Infrastructure) 42
2.15.3 IPSec............ 43
2.15.4 Java Security 44
2.15.5 Cryptography and Authentication Services 45
2.15.6 Firewalls............ 45
2.15.7 Virus Protection and E-mail Attack Countermeasures............ 48
2.15.8 S/MIME (Secure/Multipurpose Internet Mail Extensions) 48
2.16 OPEN SOURCE SOFTWARE 49

3 BEST PRACTICE EXAMPLES 50
3.1 INTRODUCTION............ 50
3.2 EIONET............ 50
3.2.1 Introduction 50
3.2.2 Technical approach 50
3.2.3 Overview of service components used by EIONET............ 52
3.3 EURES 53
3.3.1 Introduction 53
3.3.2 Technical approach 53
3.3.3 Overview of service components used by EURES 53
3.4 EUDRANET............ 54
3.4.1 Introduction 54
3.4.2 Technical approach 54
3.4.3 Overview of service components used by EudraNet............ 55
3.5 COMMUNICATION AND MANAGEMENT OF OFFICIAL DOCUMENTS 56
3.5.1 Introduction 56
3.5.2 Technical approach 56
3.5.3 Overview of service components used by CMOD............ 56

History of Document

Version	Date	Changes
Version 4.1	01/03/1999	First draft based on V.3.2.1 extended by a new chapter on IPNET (derived from the IPNET document V2.2.c).
Version 5.0	31/08/2000	Update of version 4.1, with improved structure and updated and extended information on new technologies.
Version 5.1	29/09/2000	Update of version 5.0, after processing review comments forwarded by the Commission.
Version 5.2	12/10/2000	Update of version 5.1, after processing review comments forwarded by the Commission's PAB.
Version 5.3	12/02/2001	Update of version 5.2, after processing review comments forwarded by the TAC.
Version 6.0	31/08/2001	Update of version 5.3, with roadmaps and updated and extended information on new technologies.
Version 6.1 First draft	22/10/2001	Update of version 6.0, after processing review comments forwarded by the Commission's PAB.
Version 5.1 Second draft	25/01/2002	Update of first draft of version 6.1, after processing review comments forwarded by the TAC.
Version 6.1 Third draft	01/03/2002	Update of second draft of version 6.1, after processing last review comments forwarded by the PAB and TAC.
Version 6.1 Fourth draft	28/05/2002	Update of third draft of version 6.1, after processing last review comments forwarded by the PAB.

1 Introduction

1.1 Document Structure

These annexes supplement the main document of the Architecture Guidelines to provide additional information on technical specifications (service profiles) and best practice examples.

Chapter 2 contains reference technical specifications for candidate technology (i.e. either generic services or, when available, common tools) to meet the requirements.

Chapter 3 contains a number of Best Practice Examples of projects that have implemented components of the architecture covered by these guidelines.

1.2 References

To keep the information in this document concise and in order to avoid duplication of information, details on technical standards etc are provided by means of references to external documents.

Sources from the IETF (Internet Engineering Task Force) have been applied when available. IETF guidance is referenced by RFC's (Request For Comments) and their official reference numbers are given.

It is the general IDA recommendation that IT systems should be based on:

- Formal European and International Standards.
- Standards originated in the Internet World via the work of the Internet Engineering Task Force (IETF) and W3C.
- Relevant other widely adopted information IT specifications in the public domain, referred to as Publicly Available Specifications (PAS). A PAS is a specification that meets certain criteria making it suitable for processing as an ISO/IEC International Standard.

1.3 Proprietary Products

All care has been taken to ensure that the text of these Guidelines does not make any reference to proprietary products. However, if the text does contain any explicit or implicit reference to any proprietary product, this does not in any way imply that the use of these products is required or being advised.

2 Service Profiles

2.1 Character Sets

Functionality

Character Sets are not a function in their own right, but rather a supporting component of many other IT functions or products. Most IT systems are used at some time and in some way to process information that is represented by characters, appropriate to some alphabet and natural language. When such a system has interoperability requirements with other IT systems, then these must be achieved through the application and selection of open standards relating to character sets which are appropriate for the range of natural languages to be supported.

The EuroGate must support standard character sets that are to be used for the processing and/or interchange of character-based information.

In order to avoid character set problems, Web Browsers used for WWW services over the EuroDomain should be compliant with the UTF-8 encoding of Unicode (ISO 10646).

Usage Mandatory requirement for all domains.

2.2 Document Archiving Services

Important technologies for document archiving deal with file compression, for which a number of standards have been adopted.

The transformation of data into a form that minimises the space required, as to store or transmit it, for example. One system of data compression assigns special binary codes to frequently used words so that they take up fewer bits than they would if each letter were coded separately.

2.2.1 File Compression Techniques

Functionality

File compression can speed up transmission of data by FAX machine or modem because it enables these devices to transmit the same amount of data using fewer bits. Data compression is also used in backup utilities, in storing bit-mapped graphics files, and in storing video images. A type of expansion board called a compression board will automatically compress data as it is written to disk, then decompress it when it is read. The data compression is not noticeable to the user but can effectively double or triple the capacity of a disk drive.

- Lossy compression: Data compression with some loss of information. Lossy compression can occur, for example, when data is prepared for transmission over a relatively small bandwidth. A common form of data that undergoes lossy compression is audio and video data, and the data that is lost is usually fine-resolution data whose absence is not noticeable. An example of a file format for lossy compression is JPEG.
- Lossless compression: Data compression that can be achieved with no loss of information. The currently most popular file compression formats are: ZIP, TIFF, ARC, ARJ, RAR, GZ, TAR, ACE, LZH.

For each of these compression formats shareware support tools are available via the Internet. Additionally, certain audio and video file formats imply the application of compression techniques that are the most optimal for the specific datatype, but are based on the algorithms that are also applicable for the above mentioned file compression formats.

Usage Implementation of document archiving services on a LocalDomain and exchange of documents between LocalDomains.

2.3 Document Exchange Services

Documents produced by today’s word processors have file formats that are proprietary to the word processing software used. Even though this software has built-in conversion tools that can be used to exchange documents, not all characteristics of a document will be retained as these major word processors implement highly rich features in a proprietary manner. The sender of the exchange must be fully aware beforehand of the target type of document, which makes it difficult for dissemination via a network.

If a document needs to be edited by several parties who use dissimilar word processors, it is best to exchange the document in Rich Text Format (RTF), the least common denominator between word processors and normally always available as a built-in conversion tool.

If documents have to be read at the recipient workstation as part of an Extranet dissemination platform, many other candidates are now available.

The following formats are currently used and accepted:

- PDF (Portable Document Format);
- SGML (Standard Generalised Mark-up Language);
- DSSSL (Document Style Semantics and Specification Language);
- HTML (Hypertext Mark-up Language);
- XML (eXtensible Mark-up Language);
- XMI (XML Metadata Interchange);
- UML (Unified Modelling Language);
- WebDAV.

The PDF and HTML are currently the most widely used formats for exchanging and displaying documents.

Graphics file formats can be categorised into bit-mapped formats and vector formats.

In a bit-mapped format an image is composed of a pattern of dots. This is sometimes called raster graphics. Programs that produce and manipulate bit-mapped files are called paint programs. The most common image formats for exchanging images in e-mail attachments and distributing images via web pages are GIF, TIFF and JPEG.

The vector graphics format uses geometrical formulas to represent images. Programs that produce and manipulate vector graphics are called draw programs. Vector-oriented images are more flexible than bit maps because they can be resized and stretched. In addition, images stored as vectors look better on devices with higher resolution, whereas bit-mapped images always appear the same, regardless of a device's resolution. Another advantage of vector graphics is that representations of images often require less memory than bit-mapped images do. The advised format for vector graphics is CGM.

Files can be exchanged between bit-mapped formats, vector formats, or formats that support both bit-mapped and vector graphics.

2.3.1 PDF (Portable Document Format)

Functionality

PDF is a widely used file format used to represent a document in a manner independent of the application software, hardware, and operating system used to create it. A PDF file contains a PDF document and other supporting data.

A PDF document contains one or more pages. Each page in the document may contain any combination of text, graphics, and images in a device- and resolution-independent format. This is the page description. A PDF document may also contain information possible only in an electronic representation, such as hypertext links.

In addition to a document, a PDF file contains the version of the PDF specification used in the file and information about the location of important structures in the file. The PDF is a proprietary format. However, this format has wide market acceptance and PDF or equivalent products can be used as format for document exchange within IDA because of its ease of use and features.

Usage PDF is the recommended format for distribution of formal documents between partner organisations on account of the PDF feature as a non-revisable format, providing:

- a degree of assurance on information integrity;
- consistency in layout and page numbering on all copies of a document being circulated.

2.3.2 SGML (Standard Generalised Mark-up Language)

Functionality

SGML is a standard for specifying a document mark-up language or tag set. Such a specification is itself a document type definition (DTD). SGML is a metalanguage, i.e. it is not a document language, but a description of how to specify a mark-up language.

SGML is not a document format that is well suited for open exchange of word processing documents. However, some special purpose systems (or projects) may use SGML for document interchange. The base standard for SGML is ISO 8879.

Usage Frequently used for EDI-type applications. SGML is gradually being replaced by XML.

Comments

HTML and XML are examples of SGML-based languages. There is a document type definition for HTML (reading the HTML specification is effectively reading an expanded version of the document type definition).

2.3.3 DSSSL (Document Style Semantics and Specification Language)

Functionality

DSSSL (Document Style Semantics and Specification Language) is a standard for the processing of SGML documents. Whereas SGML, which stands for Standard Generalised Mark-up Language, is a standard for describing documents in terms of logical structure (rather than presentation), DSSSL describes how such a structured document might be presented visually, or converted to something else, or processed in some other way. SGML is a document structure language; DSSSL is a document processing language, especially for presentation or transformation.

Usage see SGML

2.3.4 HTML (Hypertext Mark-up Language)

Functionality

HTML is a simple mark-up language used to create hypertext documents that are platform independent and that can be displayed by Internet browsers. HTML documents are SGML documents with generic semantics that are appropriate for representing information from a wide range of domains. HTML mark-up can represent hypertext news, mail, documentation, and hypermedia; menus of options; database query results; simple structured documents with in-lined graphics; and hypertext views of existing bodies of information.

As a document format, HTML is a good compromise for open exchange of converted word processing document except that it will not always retain all of the document structure. Most word processors include the possibility to convert a document to HTML format and also offer the possibility to read HTML documents, edit them and save them back in HTML format.

HTML is a standard recommended by the World Wide Web Consortium (W3C) and adhered to by the major browsers. HTML is an application of ISO Standard 8879:1986 Information Processing Text and Office Systems; Standard Generalised Mark-up Language (SGML).

The current version of HTML is 4.0.

Usage Generalised Web services to be set up on LocalDomains

2.3.5 XML (eXtensible Mark-up Language)

Functionality

XML is a flexible way of creating common information formats and sharing both the format and the data on the World Wide Web, intranets, and elsewhere. For example, computer manufacturers might agree on a standard or common way to describe the information about a computer product (processor speed, memory size, and so forth) and then describe the product information format with XML. Such a standard way of describing data would enable a user to send an intelligent agent (a program) to each computer maker's Web site, gather data, and then make a valid comparison.

Currently a formal recommendation from the World Wide Web Consortium (W3C). XML is similar to the language of today's Web pages, HTML. Both XML and HTML contain mark-up symbols to describe the contents of a page or file. HTML, however, describes the content of a Web page (mainly text and graphic images) only in terms of how it is to be displayed and interacted with. For example, a <P> starts a new paragraph. XML describes the content in terms of what data is being described. This means that an XML file can be processed purely as data by a program or it can be stored with similar data on another computer or, like an HTML file, that it can be displayed.

XML is "extensible" because, unlike HTML, the mark-up symbols are unlimited and self-defining. XML elements are defined in so called DTD (Document Type Definition) or in XML schema, a more powerful mechanism that describes the structure of an XML file using the same XML syntax. XML is actually a simpler and easier-to-use subset of the Standard Generalised Mark-up Language (SGML), the standard for how to create a document structure. As such, XML is emerging as standard for the exchange of a large variety of documents, including EDI messages.

Usage Web-based Presentation on LocalDomain of structured data. Increasingly used as a format for EDI-messages on account of its capability to be handled by COTS products, to support interactivity and to represent database structures.

Reference information

The complete W3C recommendation set can be found at http://www.w3.org/XML/.

2.3.6 XMI (XML Metadata Interchange)

Functionality

XMI is the proposed use of the Extensible Mark-up Language (XML) that is intended to provide a standard way for programmers and other users to exchange information about metadata (essentially, information about what a set of data consists of and how it is organised). Specifically, XMI is intended to help programmers using the Unified Modelling Language (UML) with different languages and development tools to exchange their data models with each other. In addition, XMI can also be used to exchange information about data warehouses. Effectively, the XMI format standardises how any set of metadata is described and requires users across many industries and operating environments to see data the same way.

XMI is a proposal from the Object Management Group (OMG) that builds on and extends these industry standards or recommendations:

- Extensible Mark-up Language (XML), a standard from the World Wide Web Consortium;
- Unified Modelling Language (UML), a standard from OMG;
- Meta Object Facility (MOF), another standard from the OMG for a metamodelling and metadata repository.

Usage Support of collaborative development and project documentation.

Reference information

Further information on metadata requirements can be obtained from the MOREQ project documents.

2.3.7 UML (Unified Modelling Language)

Functionality

UML is a standard notation for the modelling of real-world objects as a first step in developing an object-oriented program. Its notation is derived from and unifies the notations of three object-oriented design and analysis methodologies.

UML has been fostered and now is an accepted standard of the Object Management Group (OMG), which is also the home of CORBA, the leading industry standard for distributed object programming.

Modelling concepts of UML include: class (of objects), object, association, responsibility, activity, interface, use case, package, sequence, collaboration, and state.

Usage Support of collaborative development and project documentation.

2.3.8 WebDAV

Functionality

WebDAV (Web Distributed Authoring and Versioning allows web users in distant locations to write, edit and save shared documents without scuttling each other's work, regardless of which software program or Internet service they are using.

WebDAV enables users to save and manage documents on the web in a consistent manner. The WebDAV standard was endorsed by the IETF. The new standard offers the following key features:

- Overwrite prevention. The new standard contains a feature that prevents more than one person from working on a document at the same time. This will prevent what is known as the "lost update problem" that currently often occurs as modifications to a document are lost when multiple authors access and attempt to edit a file simultaneously. Overwrite protection will lock out all but one author at a time.
- Properties. WebDAV has developed a new, efficient means of storing and retrieving what is known as "metadata"—encoded information about a web document such as the author's name, copyright, publication date and keywords used by Internet search engines to find and retrieve relevant documents.
- Name-space management. The WebDAV standard also enables users to conveniently manage Internet files and directories, including the ability to move and copy files, similar to the way word-processing files and directories are managed on a regular computer.

Usage Collaborative web authoring.

2.3.9 GIF (Graphics Interchange Format)

Functionality

The GIF Format is a commercial format that is widely used on the web. GIF is a proprietary specification of CompuServe Information Services. GIF had been used very extensively and is widely available in almost all browsers that can handle graphics. It allows 1 bit transparency (a pixel is either transparent or opaque) and a palette of a maximum of 256 colours, so representation of 24-bit colour images in GIF involve loss of image quality.

Usage Web publishing.

2.3.10 TIFF (Tag Image File Format)

Functionality

TIFF (Tag Image File Format) is a common format for exchanging raster (bitmapped) images between application programs, including those used for scanning images. TIFF files are commonly used in desktop publishing, faxing, 3-D applications, and medical imaging applications.

TIFF files can be in any of several classes, including gray scale, colour palette, or RGB full colour, and can include files with JPEG, LZW, or CCITT Group 4 standard run-length compression.

Usage Web publishing.

2.3.11 JPEG (Joint Photographic Experts Group)

Functionality

The JPEG standard is an excellent standard for most realistic images (photos for example, but not line drawings or logos). It is a powerful, though "lossy", compression method. JPEG is best suited for true-colour original images; avoid using it on images that have already been forced into a 256-colour palette. Using JPEG for a photographic image for example can produce 10:1 savings compared to GIF, as well as permitting much better display quality on true-colour-capable displays. Many browsers handle inline JPEG; older browsers need to use an external JPEG viewer.

The JPEG standard was the result of years of effort by the Joint Photographic Experts Group which was formed as a joint effort by two large, standing, standards organisations, the CCITT (The European telecommunications standards organisation) and the ISO (International Standards Organisation.)

Usage Web publishing

2.3.12 CGM (Computer Graphics Metafile)

Functionality

The CGM format is the International Standard for storage and exchange of 2D graphical data. Although initially a vector format, it has been extended in two upwardly compatible extensions to include raster capabilities and provides a very useful format for combined raster and vector images.

The CGM file format was designed by several standards organisations and formally ratified by ANSI. It is designed to be the standard vector graphics file format and is supported by a wide variety of software and hardware products.

Four Internationally Standardised Profiles (ISPs) have been developed for CGM. CGM has been accepted as a MIME data type. CGM is being discussed by W3C as a standard for graphics on the WWW. Where vector diagrams are being sent across the network, the use of CGM would result in lower file size, faster transfer and editable files when compared with raster formats such as GIF.

Usage Web publishing.

2.4 Content Interoperability Services

2.4.1 XML-Based Standards

XML is the reference technology for most IT industry sectors (e.g. web publishing, document and knowledge management, software design, system and network management, directory interoperability, etc.) as an ideal language for defining contents to be handled, shared and exchanged. Because information is itemised and encapsulated inside custom-defined tags, carrying semantic information about data, XML provides the means for defining complex documents, made up as a set granular, manageable pieces that can programmatically be created, expanded, searched, changed, managed, linked to one another in real time, etc. Systems are designed to embed its business rules, history, usage record, etc in a documentary object. This information makes it easy to implement features such as:

- end-to-end content control – allowing users and/or applications to supervise content production;
- configuration management – the capability to maintain the correct, current baseline version of a document/document set, while making it possible to track and trace back requirements and to access previous versions of the information;
- content exchange – an XML document can be designed to carry all the business information that local user applications need to know when processing that document.
- multilingualism – XML offers designers a means of establishing the requisite level of data granularity for the contents to be handled, with ultimate capacity to set up automated translation processes, or the run-time rendering of itemised data stored in a language-independent manner.

Due to the worldwide recognition and industry support, XML is the foundation for content in trans-European networks. Applications for both information sharing and exchange should be based on related standards.

Content standardisation work on both horizontal application domains (cross-sector application interoperability, e.g. xmlCIM, DSML, etc.) and vertical application domains (interoperability of business sectors-related content) are universally adopting XML as the underlying technology for data exchange.

Usage

Use XML in the following scenarios:

- exchange of business documents between LocalDomains using a peer-to-peer communication paradigm;
- setting up web-based forms for itemised data collection;
- setting up of web content management systems that involve collaborative authoring.

Security

The XML Signature Working Group is a joint effort of the IETF (Internet Engineering Task Force) and W3C. XML Encryption WG is working on developing a process for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.

Reference information

http://www.xml.org/xmlorg_registry/index.shtml (list of initiatives in various business domains)

2.4.2 EDI Services

Functionality

Exchange of EDI messages between LocalDomains is supported by EuroDomain services. Whenever possible, exchanges should be based on UN-EDIFACT standards. However, solutions based on formats agreed within the user communities and conveyed using SGML or XML files are wide spread.

When applicable, conversion services to UN-EDIFACT messages of other standards-compliant messages (e.g. from TRADACOM - UN-EDIFACT) should be provided.

While in many cases EDI will be exchanged end-to-end through the use of messaging or file transfers, it is highly recommended that facilities such as the following are implemented:

- routing, based on UN-EDIFACT header information, i.e. the EuroDomain should be able to route EDI interchanges based on the Recipient information in UNB;
- revision track, syntax validation and syntax conversion.

EDI messages may be encapsulated using the MIME protocol. MIME is specified in detail in Internet RFC2045, RFC2046, RFC2047, RFC2048, RFC2049 and RFC2231which amend the original mail protocol specification, RFC0821(the Simple Mail Transport Protocol) and the ASCII messaging header, RFC0822, RFC1123, RFC1138, RFC1148, RFC1327, RFC2156, RFC2181 and RFC2646.

EDI messages must be based on the EN 29735:1992 (syntax). D93.A (directory services), and ISO 9735 Amendment 1:1992 (for support of Western European Character Set).

EDI messages to EDIM MSs and UAs should be based on the X.435 as defined in ISP 12063-x, with additional requirements for 84 inter-working, western European character set etc.

Usage EuroDomain, Message Transfer Services.

Security

Support ANSI X.12, EDIFACT and message handling protocol (X.400) extended to EDI (X.435).

Reference information

MIME Encapsulation of EDI Objects (RFC1767

Comments

The EEMA EDI WG is defining ways to combine XML and EDI, plus a set of specifications and Internet server-based repositories. This technology’s building blocks are XML, EDI, templates, agents and repository, playing the following role in the model:

The XML tags replace existing EDI segments or data-element identifiers. Although this produces a somewhat larger file than an EDI file, it will include all the labels of the data-elements (in other words the descriptions or explanations).

The templates are essentially rules that determine how the XML files should be interpreted. They can define the layout of the file and are supplemented by DTDs (Document Type Definitions) that enable transaction operability.

The agents can interpret the templates to perform the task to be performed, but they can also interact with the transaction and help the user to create new templates for each specific task.

The repository is a location where shared Internet directories are stored and where users can look up the meaning and definition of XML/EDI tags, either manually or automatically. The repository is in fact the semantic foundation for business transactions.

The repository is the EEMA EDI Work Group solution to giving XML/EDI a consistent, generic foundation. There is not yet any defined way to base an XML/EDI message on a unique, global and agreed repository such as UN-EDIFACT. This foundation is regarded as essential to ensure that business parties do not have to agree upon formats to set up EDI transactions.

2.5 World Wide Web (WWW) Services

2.5.1 Basic WWW Functionality

Functionality

Information stores on databases are increasingly made available through WWW technology. Secure access for well defined closed user groups to these databases can be offered by means of the advanced security features or restricted access data networks of the EuroDomain.

EuroDomain services currently include WWW hosting for LocalDomain(s) according to the HTTP protocol and HTML language based on HTML 4.0.

Usage Web-based services that are set up on a LocalDomain, or the web hosting services offered by the EuroDomain service provider.

Security

- The cgi-bin directory and its contents should be executable and readable for everybody, but can be modified only by the administrator.
- Turn on only minimal necessary functionality of the Web server for the access of the users.
- Turn symbolic link following off.
- Do not run the Web server as root or administrator.
- Do not share document tree between FTP and Web server.
- Run the server in a "chroot" environment.
- Use Dual-Homed Gateway Firewall systems.
- Use encryption such as SSL, and user authentication techniques to protect the access and transmission of confidential information.
- Use JAVA based application for dynamic web page interfaces.

Reference information

RFC2616: Hypertext Transfer Protocol – HTTP/1.1.

2.5.2 DOM (Document Object Model)

Functionality

DOM (a W3C standard) stands for Document Object Model. DOM provides a platform and language-neutral interface that is implemented in browsers, allowing scripts to dynamically access and update the content, structure and style of documents. DOM is used to provide extensive programmatic access to both HTML and XML-rendered content using JavaScript. Given an information tree embedded in an XML document, programmatic access essentially means collecting node values for processing and/or output, climbing the tree, modify values of its nodes, etc. DOM Level 2 specifies a way to manipulate and change CSS stylesheets. There is also core functionality for linking style sheets in any style sheet language to an XML or HTML file.

Usage

Both at client and server-side level.

At client level, use JavaScript within the page itself to manipulate the page or change the CSS style sheet. At server level, DOM helps develop functionality such as:

- access to database information on contents presented as a DOM tree;
- XML parsing;
- syntax transformation, XSLT processing.

Status:

- DOM Level 1 allows navigation around an HTML or XML document, and manipulation of the content in that document.
- DOM Level 2 extends Level 1 with a number of features: XML Namespace support, filtered views, ranges, events, etc.
- DOM Level 3 is underway.

Reference information

The complete W3C recommendation set can be found at http://www.w3.org/DOM/.

2.5.3 CSS (Cascading Style Sheets)

Functionality

CSS is a W3C standard that defines a style sheet language that allows authors and users to attach style (e.g., fonts, spacing, and aural cues) to structured documents (e.g. HTML documents and XML applications). By separating the presentation style of documents from the content of documents, CSS2 simplifies Web authoring and site maintenance. The specification supports content positioning, downloadable fonts, table layout, features for internationalisation, automatic counters and numbering, and some properties related to user interface.

Usage

Develop GUIs that are tailored to the audience.

Reference information

The complete W3C recommendation set can be found at http://www.w3.org.

2.5.4 XUL (Document Object Model)

Functionality

XUL, an XML-based language defining elements of a user interfaces (e.g. input controls such as text fields, toolbars with buttons or any content, menus on a menu bar or pop up menus, tabbed dialogs, trees for hierarchical or tabular information, keyboard shortcuts) that can be combined in a GUI interface, associating to any such element a process (that is implemented using JavaScript over the DOM).

XUL applications consist of XML files created with .xul extensions. The files define the content of the application. Additional application data is located in Resource Description Framework (RDF) files. CSS files provide formatting, style, and some behaviour, for the application. JavaScript files provide scripting support. Multimedia files, such as PNG images and other audio/visual files, might also be needed for additional user interface information. All of the file types are specifications recommended by the W3C, and collectively are referred to as the XUL application's "chrome" -- the contents, behaviour, and appearance of the application's user interface.

Usage

Implement complex GUIs using standard mechanisms.

2.5.5 WAI (Web Accessibility Initiative)

Functionality

As the web becomes increasingly important across all areas of society, it is vital to ensure that the web is accessible to people with disabilities, including people with visual, hearing, physical, cognitive, and neurological disabilities. Solutions developed for web accessibility often improve usability for non-disabled people as well. For instance, alternative text for images and animations benefits people with visual disabilities, but also people who access the web by mobile phones and those using slow connections. Likewise, captioning of audio not only ensures accessibility for deaf or hard of hearing users, but also increases usability of hand-held devices without audio output and audio-enabled devices used in noisy environments, and it facilitates searching for and indexing Web content.

W3C's Web Accessibility Initiative (WAI) addresses these issues through a combination of technical and educational work. As a complement to the WAI Technical Activity, WAI's International Program Office Activity maintains a general interest group on Web accessibility; develops educational material and conducts outreach activities; coordinates with research and development projects; and coordinates all areas of WAI work.

A variety of organizations participate in WAI groups. The WAI International Program Office helps create a forum where representatives of industry, the disability community, research, and government can participate together in exploring accessibility requirements and developing solutions under W3C Process. The WAI International Program Office operates the WAI Coordination Group in which Chairs of all WAI Working Groups participate. WAI is also represented on the Hypertext Coordination Group to address dependencies between Working Groups in the Interaction, Document Formats, and WAI domains.

Reference information

For more detailed information on WAI, please refer to http://www.w3.org.

2.5.6 WCAG (Web Content Accessibility Guidelines)

Functionality

The Web Content Accessibility Guidelines provide design principles for creating accessible websites. When these principles are ignored, individuals with disabilities may not be able to access the content at all, or they may be able to do so only with great difficulty. When these principles are employed, they also make web content accessible to a variety of web-enabled devices, such as phones, handheld devices, kiosks, network appliances, etc. By making content accessible to a variety of devices, the content is now accessible to people in a variety of situations.

The design principles in this document represent broad concepts that apply to all web-based content. They are not specific to HTML, XML, or any other technology. This approach was taken so that the design principles could be applied to a variety of situations and technologies, including those that do not yet exist.

Reference information

For more detailed information on WCAG, please refer to http://www.w3.org.

2.6 Middleware and Internal Interfaces

The goal of middleware is to solve the problem of sharing enterprise data across multiple, heterogeneous platforms, operating systems, servers, and client applications. A sophisticated middleware approach can speed up development and deployment and reduce costs throughout the entire development life cycle. Web-enabled middleware focuses on the translation of requests from hypertext mark-up language (HTML) or Java to database-access languages such as structured query language (SQL) through the use of a common gateway interface (CGI) script, a Web-based database application programming interface (API) like JDBC (Java database connectivity), or an information request broker approach.

The most sophisticated of the Web-based middleware approaches incorporate an "information request broker," which provides services by placing its server between the Web browser and the data. With this approach, the information request broker middleware can provide Web browser access to various types of data sources with no changes to mainframe applications.

A Web-based architecture that utilises the correct middleware, such as an information request broker approach, can provide access to various legacy platforms with no changes to the legacy application. Web-based middleware also solves the connectivity problems inherent in other middleware approaches. Careful architecture design and selection of middleware solution must be made as each form of middleware or RPC can be problematic in its operation when crossing Firewalls.

Middleware is related to all means of communications between applications and/or objects (local or remote), that connect the different parts of a distributed IT architecture and supports interoperations between remote applications. The success of Internet technology, the standardisation work done by the Object Management Group (OMG) with its Object Request Broker technology, has made middleware technology a key component in distribution and dissemination of applications via IP based networks.

Examples of middleware that are described here are:

- RPC (Remote Procedure Call);
- CGI (Common Gateway Interface);
- ORB/IIOP technology and distributed object technology;
- Distributed Application Architecture.

2.6.1 Remote Procedure Call

Functionality

RPC (Remote Procedure Call) is a protocol that a program can use to request a service from a program located in another, networked computer without having to understand network details. RPC uses the client/server model. The requesting program is a client and the service-providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned. However, the use of lightweight processes or threads that share the same address space allows multiple RPCs to be performed concurrently.

There are several RPC models and implementations. A popular model and implementation is the Open Software Foundations' Distributed Computing Environment (DCE). The IEEE defines RPC in its ISO Remote Procedure Call Specification, ISO/IEC CD 11578 N6561, ISO/IEC, November 1991. RPC spans the transport layer and the application layer in the Open Systems Interconnection (OSI) model of network communication. RPC makes it easier to develop an application that includes multiple programs distributed in a network.

Usage To integrate distributed processes on Local Domains.

Comments

RPC: Remote Procedure Call Protocol Specification Version 2: RFC1831

2.6.2 CGI (Common Gateway Interface)

Functionality

CGI, the common gateway interface is a standard way for a Web server to pass a Web user's request to an application program and to receive data back, to be forwarded to the user. When the user requests a Web page (for example, by clicking on a highlighted word or entering a Web site address), the server sends back the requested page. However, when a user fills out a form on a Web page and sends it in, it usually needs to be processed by an application program. The Web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method or convention for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the Web's HTTP protocol.

Because the interface is consistent, a programmer can write a CGI application in a number of different languages. The most popular languages for CGI applications are: C, C++, Java, and Perl.

FastCGI is a programming interface that can speed up Web applications that use the most popular way to have the Web server call an application, the common gateway interface. FastCGI is a plug-in to the Web server. It requires only small changes to existing server applications (such as Perl or Tcl scripts and C and C++ programs) to get the performance benefits.

FastCGI is language-independent. It was developed and is copyrighted by Open Market, Inc., which makes it freely available and offers it as an open standard. It offers a single non-proprietary approach for use across platforms and on any Web server

PHP - As an alternative to JSP, PHP can be used as a server-parsed scripting language for use to web-enable applications that are designed to run on a LocalDomain. PHP is an open-source server-parsed embedded scripting language. Like JSP (and the competing Microsoft ASP technology), PHP is based upon the paradigm of embedding programming code within the HTML that makes up a web page. The web server interprets and executes this code, replacing the code with its results, and delivering the resulting web page to the browser. PHP's shortcoming is that PHP can only be used on web servers that provide explicit PHP support, unless it is used as any CGI script, where the web server passes the code on to a PHP interpreter (the CGI wrapper method works with a wide variety of web servers, but is not efficient in execution speed and resource consumption).

ISAPI (Internet Server Application Program Interface) is a set of Windows program calls that let a Web server application run faster than a Common Gateway Interface (CGI) application. A disadvantage of a CGI application (or "executable file," as it is sometimes called) is that each time it is run, it runs as a separate process with its own address space, resulting in extra instructions that have to be performed, especially if many instances of it are running on behalf of users.

Usage: To provide web access to a database run on a LocalDomain.

2.6.3 CORBA

Functionality

CORBA is an architecture and specification for creating, distributing, and managing distributed program objects in a network. It allows programs at different locations and developed by different vendors to communicate in a network through an "interface broker." CORBA was developed by a consortium of vendors through the Object Management Group (OMG), which currently includes over 500 member companies. Both ISO and X/Open have sanctioned CORBA as the standard architecture for distributed objects (also known as components). CORBA 2.0 is the latest level.

The essential concept in CORBA is the Object Request Broker (ORB). ORB support in a network of clients and servers on different computers means that a client program (which may itself be an object) can request services from a server program or object without having to understand where the server is located in a distributed network or what the interface to the server program looks like. To make requests or return replies between the ORBs, programs use the General Inter-ORB Protocol (GIOP) and, for the Internet, its Internet Inter-ORB Protocol (IIOP). IIOP maps GIOP requests and replies to the Internet's Transmission Control Protocol (TCP) layer in each computer.

Usage: To develop distributed trans-European network applications.

Comments

Inter-domain distributed applications should not be considered for the security implications of having application binding components through LocalDomain firewalls.

Reference OMG CORBA specifications can be accessed at http://www.omg.org

DCE, a distributed programming architecture that preceded the trend toward object-oriented programming and CORBA is currently used by a number of large companies. DCE will perhaps continue to exist along with CORBA and there will be "bridges" between the two.

2.6.4 Distributed Application Architecture

J2EE is the reference set of specifications for distributed application design, development and deployment in the area of the IDA architecture.

J2EE provides a three-tiered application model, not necessarily Web-based, that within the IDA architecture always includes a web-based interface to enable ubiquitous access. At the client tier, a user's web browser downloads static or dynamic Hypertext Markup Language (HTML) or Extensible Markup Language (XML) web pages. Some implementations might include serving up WAP pages to WAP-enabled mobile browsers.

Under certain circumstances and in line with rules defined in the current version of the Guidelines, web pages downloaded from the web tier can include an embedded applet. An applet is a small client application written in the Java programming language that executes in the Java VM installed in the web browser.

J2EE web components can be either JSP pages or servlets. Servlets are Java programming language classes that dynamically process requests and construct responses. JSP pages are text-based documents that execute as servlets, but allow a more natural approach to creating static content.

The business tier provides the application logic handled by Enterprise Java Beans (EJB).

Finally, the enterprise information system tier handles enterprise information system software, and includes enterprise infrastructure systems such as database systems, mainframe transaction processing and other legacy information systems. J2EE application components need to access enterprise information systems for database connectivity.

Below the J2EE specifications are described in more detail:

1) Enterprise JavaBeans Technology 2.0	The EJB specification defines an architecture for the development and deployment of transactional, distributed object applications-based, server-side software components using Java as the underlying language. EJB is used to build the business logic component in the IDA three-tiered model. An EJB as a building block that can be used alone or with other EJBs to execute business logic on a J2EE server. An EJB receives data from client programs, processes it, and sends it to the Enterprise Information System (EIS) tier for storage. An EJB retrieves data from storage, processes it and sends it back to the client program. Organisations can build their own components or purchase components from third-party vendors. EJB server-side components, called enterprise beans, are distributed objects that are hosted in Enterprise JavaBean containers and provide remote services for clients distributed throughout the network. EJBs communicate with each other using Java Remote Method Invocation (RMI) over the CORBA Internet InterOrb Protocol (IIOP). There are three kinds of enterprise beans: session beans, entity beans, and message-driven beans. A session bean represents a transient conversation with a client. When the client finishes executing, the session bean and its data are removed. An entity bean represents persistent data stored in one row of a database table. An entity bean gives access to a database with no need to write any SQL code (using JDBC API): if the client terminates or if the server shuts down, the underlying services ensure the entity bean data is saved. A message-driven bean combines features of a session bean and a Java Message Service (JMS) message listener, allowing a business component to receive JMS messages asynchronously.
2) JDBC 2.0 API	JDBC is an API specification for connecting programs written in Java to the data in RDBMS platforms. The application program interface lets developers encode access request statements in structured query language (SQL) that are then passed to the program that manages the database. It returns the results through a similar interface. JDBC is used to perform SQL statements:

	• In an entity bean if the container-managed persistence is to be overridden; • In a session bean if access to a database is needed; • In a Servlet or a JSP page to access the database directly without going through an enterprise bean. JDBC actually has two levels of interface. In addition to the main interface, there is also an API from a JDBC "manager" that in turn communicates with individual database product "drivers", the JDBC-ODBC bridge if necessary, and a JDBC network driver when the Java program is running in a network environment (that is, accessing a remote database). When accessing a remote database, JDBC takes advantage of the Internet's file addressing scheme and a file name looks much like a Web page address (URL). JDBC specifies a set of object-orient programming classes for the programmer to use in building SQL requests. An additional set of classes describes the JDBC driver API. The most common SQL data types, mapped to Java data types, are supported. The API provides for implementation-specific support for transactional requests and the ability to commit or roll back to the beginning of a transaction.
3) Java Servlet Technology 2.3	The Servlet technology lets implementers define Java plug-ins for web servers, offering a request-response programming model. With Servlets, Web server extensions are written that in response to HTTP perform Java code (commonly, calling an EJB to run some business logic or to access a database).
4) JavaServer Pages (JSP) Technology 1.2	A JSP page brings together static and dynamic contents during web browser interaction with a web server, enabling Java expressions and code to be intermixed with text-based contents. A JSP page is a text document combining static template data expressed in any web text format (such as HTML, WML and XML) and JSP-specific statements to constructs dynamic content.
5) Java Message Service (JMS) 1.0	Message-Oriented-Middleware (MOM) provides a reliable way for programs to create, send, receive and read messages in distributed system. MOM ensures reliable asynchronous communication, guaranteed message delivery, receipt notification and transaction control. Messaging systems are classified into different models that determine which client receives a message. The most common messaging models provide support for the following models: **Publish-subscribe Messaging** – this is used when multiple applications need to receive the same messages. The basic concept to publish-subscribe messaging is the Topic. Multiple publishers may send messages to a Topic, and all subscribers to that Topic receive all the messages sent to that Topic. **Point-to-Point Messaging or Message Queue** – this is used when one process needs to send a message to another process. There are two basic types of point-to-point messaging systems: the first one involves a client that directly sends a message to another client; the second and more common implementation is based on the concept of a Message Queue. **Request-Reply Messaging** – this is used when an application sends a message and expects to receive a message in return. This is the standard synchronous object-messaging format. This messaging model is often defined as a subset of one of the other two models. Java Message Service (JMS) is the market standard providing a standard Java-based interface to multi-vendor message services. The JMS API is a messaging standard that allows J2EE application components to create, send, receive, and read messages. It enables distributed communication that is loosely coupled, reliable, and asynchronous. The JMS interface is implemented on top of a messaging system. JMS defines both queues (Point-to-Point Messaging model)

	and topics (Publish-Subscribe Messaging model) as the target for a message. Commercial implementations commonly support: • bi-directional non-repudiation; • guaranteed message delivery; • process check-point restart; • communications service failover; • two-phase commit process completion; • failure recovery; • both synchronous and asynchronous communications supporting connections such as FTP, SMTP/POP3, HTTP and IIOP.
6) Java Transaction API (JTA) 1.0	Middleware implementing transaction services provide the means to build multiple, distributed objects that cooperate through the notion of managed transaction, resulting in a coherent unit of work with features such as: atomicity (if interrupted by failure, all effects are undone); consistency of results; isolation (a transaction's intermediate states are not visible to other transactions); persistency. A transaction can be terminated in two ways: the transaction is either committed or rolled back. When a transaction commits, all changes made by the associated requests are made permanent. When a transaction rolls back, all changes made by the associated requests are undone. The Transaction Service enables the objects to either commit all changes together or to rollback all changes together, even in the presence of failure. No requirements are placed on the objects other than those defined by the Transaction Service interfaces. In commercial products, the Object Transaction Service (OTS) is seen by clients using an object class that allows clients to start, join, suspend, resume, complete, and destroy transactions. The Object Transaction Service-compliant interfaces are available to any application or server. Application developers do not need to be concerned with the mechanics of distributed transaction management. The transaction propagation and recovery machinery is handled automatically. The platform provides transaction-tracking services, load balancing, recovery services, and the ability to restart servers and queues automatically. JTS (Java Transaction Service) is the current market standard for these Guidelines. JTS is designed to ensure interoperability with sophisticated transaction resources such as transaction processing monitors and transaction managers. JTS provides an open standard access method to these transaction resources for different vendors. Java Transaction Service (JTS) specifies the implementation of a Transaction Manager which supports the Java Transaction API (JTA) 1.0 Specification at the high-level and implements the Java mapping of the OMG Object Transaction Service (OTS) 1.1 Specification at the low-level. JTS uses the standard CORBA ORB/TS interfaces and Internet Inter-ORB Protocol (IIOP) for transaction context propagation between JTS Transaction Managers. A JTS Transaction Manager provides transaction services to the parties involved in distributed transactions: the application server, the resource manager, the standalone transactional application, and the Communication Resource Manager (CRM).

7) JavaMail Technology 1.2	The J2EE platform includes the JavaMail API with a JavaMail service provider that application components can use to send and receive Internet mail, e.g. to include in applications functionality for sending e-mail notifications. This API allows Java applications and EJB components to access e-mail systems using POP3 or IMAP.
8) Java API for XML (JAXP) 1.1	JAXP enables the reading, manipulating, and generating of XML documents through Java APIs, by providing a standard way to seamlessly integrate any XML-compliant parser with a Java technology-based application. JAXP v. 1.1 supports the latest XML standards, including the Document Object Model (DOM) level 2, a World Wide Web Consortium (W3C) recommendation that was released in April 2001; Simple API for XML (SAX) level 2, the industry standard for XML parsing; and Extensible Stylesheet Language Transformations (XSLT), an integrated XML transformation standard defined by the W3C. With JAXP, developers have the flexibility to swap XML parsers depending on the needs of the application, without actually changing any code. One XML parser available is Crimson, which Sun developed and donated to the Apache Software Foundation. It is the default XML parser with JAXP v. 1.1; however, the technology's plug-and-play architecture allows the use of any XML-conformant parser, including the Apache Software Foundation's code-named Xerces, or Xerces 2, a best-of-breed parser now in development.
9) J2EE Connector API 1.0	The Connector API is used by J2EE tools vendors and system integrators to create resource adapters that support access to enterprise information systems that can be plugged into any J2EE product. A resource adapter is a software component that allows J2EE application components to access and interact with the underlying resource manager. Because a resource adapter is specific to its resource manager, there is typically a different resource adapter for each type of database or EIS.
10) Java Authentication and Authorisation Service (JAAS) 1.0	The Java Authentication and Authorisation Service (JAAS) provides a way for a J2EE application to authenticate and authorise a specific user or group of users to run it. JAAS is a Java programming language version of the standard Pluggable Authentication Module (PAM) framework that extends the Java 2 platform security architecture to support user-based authorisation.
Java Security	Please refer to section 2.15.4.

2.6.5 Internal Interfaces

Functionality

To ease the development (and thus reduce costs) of the transit function or the adaptations or conversions needed for the LocalDomain, Application Program Interfaces (APIs) should be available at the EuroGate.

The strongest APIs are, for the moment, the de facto APIs (X/Open), since the formal standardisation of APIs only began a few years ago. However, standardisation of the APIs is rapidly being finalised and profiled by bodies such as:

- IEEE;
- Regional Workshops on Open Systems (EWOS, AOW, OIW).

The APIs developed by IEEE are being submitted to ISO for formal standardisation. Also, X/Open has well-defined interfaces to IEEE, and hence their work can be progressed to formal standardisation. It should also be noted that X/Open's Standards Policy is similar to the one in the 87/95 Council Decision (i.e. to use formal standards if they exist).

The following standardised APIs are relevant:

• Message Transfer Service: IEEE P1224.1	IEEE
• Directory Services: IEEE P1224.2	IEEE
• File Transfer: IEEE P1238.2	IEEE
• Distributed Transaction Processing	XATMI, TxRPC, CPI-C, XA, XA+, TX, XA-TP.X/Open
• Transport Service: XTI	X/OPen

Usage EuroGate, Middleware and Internal Interfaces

2.7 Message Transfer Services

Messaging Services are supported in the form of a Message Transfer System (MTS), in accordance with the following protocols:

- X.400
- SMTP
- EDI services
- MIME

The Message Transfer Services must support the exchange of binary attachments, and multiple body parts.

For the EuroDomain, performance requirements should be established and agreed in contracts with EuroDomain service providers. Since a Messaging Service is generally available as a means of accessing any LocalDomain, the LocalDomain (or its EuroGate) should support a minimum Messaging Service allowing the reception of basic messages.

2.7.1 X.400

Functionality

In the case of X.400 message transfer, the EuroGate is a Message Transfer Agent. The relevant protocol is therefore the X.400 P1 protocol.

Usage To support exchange of business documents between LocalDomains.

Security

The security features provided by the MHS apply only to messages submitted directly to an MTA by an MTS user. They do not apply to communication between the MHS user (e.g., a person) and the MHS (e.g., the person's UA). Thus, the scope of MHS security services extends, for example, to communication between two UAs, but not to communication between two people. Many of the MHS security services require security capabilities within the UA, but not the MTA.

Reference information

- Recommendations for the Phase I Deployment of OSI Directory Services (X.500) and OSI Message Handling Services (X.400) within the ESnet Community (RFC1330).
- Mapping between X.400 (1988) / ISO 10021 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156).
- Equivalence between 1988 X.400 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156) Message bodies: RFC2156.
- Rules for Downgrading Messages from X.400/88 to X.400/84 When MIME Content-Types is Present in the Messages: RFC1496.
- Use of the X.500 Directory to support mapping between X.400 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156): RFC2156. Addresses (RFC2164).

Comments

X.400 is gradually being replaced by the SMTP protocol which works over the TCP/IP protocol.

If the EuroDomain uses X.400 and LocalDomains use SMTP as their mail standard, a SMTP/X.400/SMTP conversion should be provided. Taking into consideration that bandwidth requirements will grow tremendously in the next few years, the trend towards SMTP is irreversible.

2.7.2 SMTP

Functionality

SMTP (Simple Mail Transport Protocol) is a TCP/IP protocol used for sending and receiving e-mail and is usually implemented to operate over TCP port 25.

In the case where LocalDomains are using the SMTP mail protocol internally, the EuroGate should provide an SMTP/X.400/SMTP conversion mechanism that will allow a LocalDomain to use the X.400 Messaging Transfer protocol used by the EuroDomain to transfer and receive messages with other LocalDomains.

Usage To support exchange of business documents between LocalDomains.

Security

- Use of a firewall system is required to secure e-mail transactions between the external world and the internal network (see Chapter2.15.6, Firewalls).
- Improve SMTP security with *smap* and *smapd.*
- Use of a firewall can protect against command channel attacks by restricting the number of machines to which attackers can open command channels and by providing a secure server on those machines.
- Run up-to-date delivery and user agents and do educate your users against data-drive attacks.
- Use automatic antiviral software updated on a regular basis. This antiviral software could be hosted on a server at the EuroGate where SMTP/X400/SMTP gateways take places. A concept of decontamination zone can then be implemented with off the shelf software. Contaminated messages are then not routed to their final destination but blocked at EuroGate level.

Reference information

- SMTP: RFC0821.
- Mapping between X.400 (1988) / ISO 10021 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156).
- Equivalence between 1988 X.400 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156) Message bodies: RFC2156.
- Rules for Downgrading Messages from X.400/88 to X.400/84 When MIME Content-Types is Present in the Messages: RFC1496.
- Use of the X.500 Directory to support mapping between X.400 and RFC0822 (and applied updates: RFC1123, RFC1138, RFC1148, RFC1327, RFC2156) Addresses (RFC2164).

2.7.3 Message Store Services

Functionality

The EuroGate may provide a Message Store Service, based on the X.400-P7 recommendations and/or IMAP4 protocols according for TCP-IP based services to the LocalDomain. This service may be offered to end-users, based on LAN connections, or access through dial-up connection.

In case of use of IMAP4 protocol, file attachments are received and sent according to the MIME protocol defined in RFC2045, RFC2046, RFC2047, RFC2048, RFC2049 and RFC2231.

Usage EuroDomain.

Security

- IMAP4 Authentication Mechanisms (RFC1731).

Reference information

- Internet Message Access Protocol - Version 4 (RFC2060 and RFC2061).
- File attachment for IMAP4 are received and sent according to MIME protocol defined in RFC2045, RFC2046, RFC2047, RFC2048 and RFC2049.
- Recommendations for the Phase I Deployment of OSI Directory Services (X.500) and OSI Message Handling Services (X.400) within the ESnet Community (RFC1330).

2.7.4 MIME

Functionality

MIME (Multi-Purpose Internet Mail Extensions) is an extension of the original Internet e-mail protocol that lets people use the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII handled in the original protocol, the Simple Mail Transport Protocol (SMTP). In 1991, Nathan Borenstein of Bellcore proposed to the Internet Engineering Task Force that SMTP be extended so that Internet (but mainly Web) clients and servers could recognise and handle other kinds of data than ASCII text. As a result, new file types were added to "mail" as a supported Internet Protocol file type.

Servers insert the MIME header at the beginning of any Webtransmission. Clients use this header to select an appropriate "player" application for the type of data the header indicates. Some of these players are built into the Web client or browser (for example, all browsers come with GIF and JPEG image players as well as the ability to handle HTML files); other players may need to be downloaded.

New MIME data types are registered with the Internet Assigned Numbers Authority (IANA).

MIME is specified in detail in Internet RFC1521 and RFC1522, which amend the original mail protocol specification, RFC0821 (the Simple Mail Transport Protocol) and the ASCII messaging header, RFC0822.

2.8 File Transfer Services

File Transfer Services are supported by the EuroDomain Carrier Services in a transparent manner. In general, file transfers occur end-to-end with no functional involvement of the EuroDomain.

2.8.1 FTP and HTTP protocol

Functionality

FTP applications must comply with the current standard as defined in RFC959. The updates to this standard, as defined in RFC2228 and RFC2640, should also be taken into account.

Usage To support data collection/distribution models.

Security

- If FTP is authorised, all types of files should be thoroughly checked against any viruses with the best antiviral software available,
- Use of the known FTP:// sites, a list of authorised FTP sites could be maintained at Firewall and/or router level and all other FTP:// requests refused.
- The server SHOULD confirm that the network address of the remote hosts on both the control connection and the data connection are within the organisation before sending a restricted file.
- After a small number of attempts (3-5), the server SHOULD close the control connection with the client. In addition, the server should impose a 5 seconds delay before replying to an invalid "PASS" command.
- If you are providing anonymous FTP service, the challenge is to ensure that the anonymous FTP server makes available only the information that you want made available and that it doesn't give an outsider access to other, supposedly private, information on the machine.
- The servers should not open data connections to TCP port number below 1024.
- If a server receives a PORT command containing a TCP port number less than 1024, the response should be 504 (defined as "Command not implemented for that parameter" by [41]).
- All HTTP downloaded files should be treated with the same precautions as all FTP downloaded files.
- If using a net browsing-program, *disable* automatic launching of the active agents.
- For security critical systems, usage of the browsing-programs should be under strict control or even forbidden.

2.9 Workflow Management

Standards in the area of workflow management are taken from the results of the Workflow Management Coalition.

2.9.1 Workflow Management Coalition

General information

The Workflow Management Coalition is a non-profit, international organisation of workflow vendors, users, analysts and university/research groups. The Coalition's mission is to promote and develop the use of workflow through the establishment of standards for software terminology, interoperability and connectivity between workflow products. Consisting of over 275 members, spread throughout the world, representing all facets of workflow, from vendors to users, and from academics to consultants, the Coalition has quickly become established as the primary standards body for this rapidly expanding software market.

The initial work of the Coalition focused on publishing the Reference Model and Glossary, defining a common architecture and terminology for the industry. A major milestone was achieved with the publication of the first versions of the Workflow API (WAPI) specification, covering the Workflow Client Application Interface, and the Workflow Interoperability specification. The Audit Data specification was added in 1997, being followed by the Process Definition Import/Export specification.

A further version of WAPI covers Application Invocation API's, completing the Coalition's initial deliverables across the five interface functions. Further work includes the completion of a common object model with object bindings for IDL and OLE, interoperability extensions for security, and additional interoperability models.

Important Specifications

- Interoperability, Wf-XML Binding (WFMC-TC-1023) - This specification is intended for use by software vendors, system integrators, consultants and any other individual or organisation concerned with interoperability among workflow systems. Furthermore, it will be of value to those concerned with the design and implementation of integrated and/or distributed systems, as a protocol for the interaction of generic (possibly remote) services.
- Workflow Standard Interoperability, XML-HTTP Binding (WFMC-0208) - This document represents a workflow protocol that aims for interoperable, reliable, and practical interactions between services using HTTP protocol. This protocol is based on Wf-XML and extended for the sake of enterprise EDI applications. As a result, Wf-XML is proved to be useful for developing EDI systems. However, some tags and interfaces needed to be added to Wf-XML because Wf-XML falls short of some essential functions for EDI systems, that is, asynchronous messaging and multiple messaging.
- Workflow Security Considerations, White Paper (WFMC-TC-1019) - The document summarises a number of security services that may be important within a workflow system and relates them to a generalised model identifying different security domains within a heterogeneous workflow environment. It then identifies areas of potential work for the WfMC, concentrating on Workflow interoperability between different organisational domains.

2.10 Directory Services

It is assumed that the Directory Service will be distributed, i.e. that each EuroGate will provide access to the directory information regarding the LocalDomain.

The following two solutions are available:

- X.500
- LDAP

The EuroDomain should provide a Directory Access Service that should interconnect X.500 Directory Services in the LocalDomains or in the EuroGates on behalf of the LocalDomains. The Directory Service should support user access through the Directory Access Protocol (DAP).

The EuroDomain Directory Service should be interconnected with external X.500 or LDAP Directory Services of an international or national nature.

The directory services offered to EuroDomain participants should evolve to an architecture based on LDAP servers located at the EuroGate with X.500 directory access where needed. In turn these LDAP servers could then be accessed by LDAP enabled client applications located in LocalDomains.

The EuroGate or the LocalDomain(s) should make directory information available in sufficient detail to allow the EuroDomain Directory Service to function. Users in other LocalDomains must be able to obtain, via the EuroDomain Directory Service, information on names and addresses intended to be available from this LocalDomain.

2.10.1 X.500

Functionality

X.500 provides a viable distributed solution for white pages information on the Internet and the only one demonstrated so far. It is the only open set of standards that defines protocols, replication, security and an information model.

Usage EuroDomain.

Security

- An *authentication attribute*, such as a password, can be included with an entry (simple authentication).
- In more security demanding applications the *strong authentication* should be employed (private/public key mechanism.

Reference information

- Naming and Structuring Guidelines for X.500 Directory Pilots (RFC1617).
- Technical Overview of Directory Services Using the X.500 Protocol (RFC1309).
- A Survey of Advanced Usage of X.500 (RFC1491).
- Representing IP Information in the X.500 Directory (RFC1608).
- A Strategic Plan for Deploying an Internet X.500 Directory Service (RFC1430).

Comments

- DUAs shall support the DAP protocol as specified in ISO/IEC 9594 parts 3 and 5, and in respect of distributed operations, shall conform with ISP 10615-5. They shall be able to create and make rendition of names, attributes, and object classes as defined by ISP 10616.
- DSAs participating in distributed operations shall support the DAP protocol specified in ISO/IEC 9594 parts 3 and 5, the DSP protocol specified in ISO/IEC 9594 parts 4 and 5, together with the Functional Standards specified in ISP 10615 parts 2, 3, 4 and 6 and ISP 10616.
- DUAs shall support DAP protocol as specified in ISO/IEC 9594 parts 3 and 5. They shall be able to create and make rendition of names, attributes, and object classes as defined by ISP 10616. For centralised Directory systems, the DSA shall support the DAP protocol specified in ISO/IEC 9594 parts 3 and 5, and the Functional Standards specified in ISP 10615-2 and ISP 10616. The DSA shall also be capable of extension to distributed operations, and thus shall support the DSP protocol specified in ISO/IEC 9594 parts 4 and 5, together with the Functional Standards specified in ISP 10615 parts 3, 4 and 6. The root of any DIT sub-tree supported by the DSA shall not be required to be immediately subordinate to the root of the DIT.
- General purpose DUAs and DSAs must comply with at least the minimum requirements for handling APDU size, string lengths for filters and filter items defined by ISP 10615-2, ISP 10615-3 and ISP 10615-4.
- DSAs conforming to the 1988 base standard shall support the rules for extensibility for operation processing as specified in ISP 10615-3 and ISP 10615-4.

2.10.2 LDAP

Functionality

The Lightweight Directory Access Protocol (LDAP) is a strategic directory protocol for the future (See RFC1777, "Lightweight Directory Access Protocol"). Based on a client-server model, it defines a reasonably simple mechanism for Internet clients (or Intranet and Extranet clients), to query and manage an arbitrary database of hierarchical attribute/value pairs over a TCP/IP connection (port 389). LDAP, a simplification of the X.500 directory access protocol (DAP), is also gaining significant Internet support, including the support of many significant companies and has been universally welcomed and endorsed by all the leading industry players.

Recent innovations suggest that an Internet URL definition for LDAP searches could be quite useful. This URL representation not only identifies the protocol (LDAP) but also encodes the DNS host name.

It is also possible to integrate LDAP and existing DNS servers by adding a record to an existing DNS server that points LDAP URLs to an LDAP server within the domain. The reverse is also possible: a corporation can add DNS entries to their internal LDAP server so that failing local searches can be referred over DNS to distant LDAP servers.

Usage EuroDomain.

Security

- In systems with high security level requirements, the DAP protocol with the appropriate data encryption should be considered.
- Any program that makes authentication or authorisation decisions based on the host name information it gets from DNS should be very careful to validate the data with the reverse lookup/double-reverse lookup method.
- Use an up-to-date version of the DNS software.
- Hide internal DNS information to the external world.
- The DNS service should not collide with Internet DNS names or addresses (RIPE).

Reference information

- LDAP Version 3 – RFC1777, RFC2251, RFC2553 and RFC2559.
- A Summary of the X.500 (96) User Schema for use with LDAPv3 (RFC2256).
- Use of an X.500/LDAP directory to support MIXER address mapping (RFC2164).
- The LDAP Application Program Interface (RFC1823).

Comments

LDAP is purely a lightweight alternative to the X.500 access protocol. It does not address how the directory service itself is structured. This is why X.500 is important - it provides a proven blueprint for implementing a directory service.

LDAP is a simple and popular way of accessing this service. Standalone LDAP servers offer a common API and protocol amongst heterogeneous directory servers. Many of the standalone servers “borrow” ideas and concepts from X.500, but do not adopt them in such a way as to provide compliance with the X.500 standards. Hence it appears at the moment that numerous heterogeneous directory systems are available with varying degree of conformity to X.500. Their only common ground is the support for the LDAP protocol and API.

2.11 Network Management Services

Selected resources at the EuroGates act as OSI Management Agents, reporting events to, and being controlled from, a management point.

2.11.1 SNMP

Functionality

The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

Usage EuroDomain, Network Management Services

Security

- User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (RFC2574).
- Use a message digest algorithm to support data integrity.
- Use a timestamp value in each message generated to avoid message reordering.
- Use a symmetric encryption algorithm to support data confidentiality.

Reference information

- Simple Network Management Protocol Distributed Protocol Interface (RFC1592).
- Message Processing and Dispatching for SNMP (RFC2572).
- An Architecture for Describing SNMP Management Frameworks (RFC2571).
- Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) (RFC2578).
- Management Information Base for Network Management of TCP/IP-based internets: MIB-II (RFC2011, RFC2012 and RFC2013).
- Conformance Statements for Version 2 of SNMP (SNMPv2) (RFC2580).

Comments

- The implementation must conform to all the mandatory requirements for the manager role of profiles AOM211, AOM221 and AOM231 as specified by ISO/IEC ISP 12060-1, 12060-4 and 12060-5 respectively.
- The implementation must conform to all the mandatory requirements for the agent role of profiles AOM211 and AOM221 as specified by ISO/IEC ISP 12060-1 and 12060-4 respectively and of profile AOM231 as specified by ISO/IEC ISP 12060-5.
- All *managed objects* provided or used by suppliers, whether standardised or not, must be defined in accordance with ISO/IEC 10165-1 (the Management Information Model), use the tools specified in ISO/IEC 10165-4 (Guidelines for the Definition of Managed Objects), and include Implementation Conformance Statements as required by ISO/IEC 10165-6 (Requirements and Guidelines for ICS Proformas related to OSI Management).
- The implementation must conform to all the requirements for the peer entity authentication option in agent role or manager role (as appropriate) of profile AOM211 as specified by ISO/IEC ISP 11183-1 as referenced from ISO/IEC ISP 12060-1.
- The implementation must conform to all the requirements for Systems Management Functional Unit Negotiation of profile AOM211 as specified by ISO/IEC ISP 12060-1.

2.11.2 Directory-Based Management Services

Functionality

On trans-European networks consider implementing an LDAP-based directory service to provide users with managed information tools for:

- looking up addresses and other information about people and other entities, either using a directory search engine or using an application (such as an e-mail client) that queries the directory;
- creating, securing, and sending e-mail messages;
- receiving e-mail messages;
- obtaining other users' certificates from the Directory for secure messaging;
- looking up certificates and CRLs in order to verify both other users' certificates for secure messaging and the server's certificate;
- accessing information;
- using services and applications;
- roaming to different local environments.

System and network management

For directory-based system and network management, refer to DMTF's Directory Enabled Networks (DEN) working group specifications, including:

- CIM Specification v2.2: (the language and methodology for describing data management);
- SIM Schema v2.2: (defining models for enabling applications from different developers on different platforms to describe management data in a standard format. CIM Schema v2.2 includes models for logical networks, to complete the DEN model, and Distributed Application Processing (DAP);
- XML Mapping v2.0 and XML DTD v2.0: the XML Mapping specification defines a standard for the representation of CIM elements and messages in XML. XML Mapping v2.0 now includes additions for HTTP operations.

Usage To support storage and retrieval of service information in designated application areas.

Security See current table on LDAP.

Reference information

The directory server solution should conform to the IETF Lightweight Directory Access Protocol (LDAP) version 3. LDAP Certification according to most current OpenGroup programs is recommended – the requirements are fully described in the Product Standard at:

http://www.opengroup.org.

Server specification:

- Meet the mandatory requirements for a server of IETF RFC2251 (Lightweight Directory Access Protocol version 3), of RFC2252 (Attribute Syntax Definitions), and of RFC2253 (UTF-8 String representation of Distinguished Names).
- Return referrals and continuation references as described in RFC2251, and in conformance with the mandatory requirements of RFC2254 (The String Representation of LDAP Search Filters) and IETF RFC2255 (The LDAP URL Format) when returning LDAP URLs in referrals and continuation references.
- Implement the mapping of LDAP over TCP described in Section 5.2.1 of RFC2251 in which the LDAP messages are mapped directly onto a TCP byte stream.

- Conform to the mandatory requirements for a server of the Secure Sockets Layer Protocol (SSL), version 3.
- Implement a mapping of LDAP over TCP in which the LDAP messages are mapped directly onto an SSL byte stream.

The following optional features of LDAP version 3 can be supported:

- extensible match;
- notice of disconnection;
- client modification of subschema entries;
- validation of client SSL certificates;
- access to SSL credentials via SASL EXTERNAL..

Comments

LDAP v.3 compliant commercial platforms and products should be chosen that provide the following centralised directory administration features:

- configure directory schema;
- add, modify and delete entries;
- define directory access control;
- configure replication between directories;
- configure referrals, chaining, replication, and other server-server communication mechanisms to federate directories;
- capability for users to add, modify and delete “own” directories.

2.12 Group Working

Group working tools support the collaboration of different teams, work groups and committees, in particular by means of the electronic management and exchange of documents.

Most of the time, the documents to be exchanged are documents created by the basic office tools (word processing, spreadsheet and presentation programmes). These could be simple notes, agendas, minutes of meetings, papers, reports and presentations. Other types of information that needs to be exchanged are e-mail addresses, Web-site links, meta-data on documents etc.

A common tool that is currently available and that was developed under the IDA Programme is CIRCA (Communication and Information Resource Centre Administrator). CIRCA is an Internet based tool for dissemination and workgroup communication. It features structured access control ("what you see is what you are allowed to access"), information pages, a document library, a user directory, meeting support (including virtual meetings) and much more, organised on an Interest Group base.

2.13 Carrier Telecommunication Services

The Carrier Services are defined as the basic transmission system (i.e. OSI layers 1-3.).

2.13.1 Circuit Switched Services, ISDN

Functionality

ISDN is used as a service to access the EuroDomain. The ISDN recommendations used in LocalDomain may vary from the EuroDomain's service. In order to function reliably and as intended, the EuroGate or the LocalDomain(s) should provide ISDN conversion mechanisms to allow LocalDomain(s) to interact with EuroDomain's Euro-ISDN service. The service should be available and compatible on a cross-European scale.

ISDN should be available in the form of ISDN-2 (2x64 kbps lines) and ISDN-30 (with 30x64 kbps lines).

ISDN is characterised by a large number of standards: over two hundred apply to public and private ISDN. For convenient communications, the European Telecommunications Standards Institute (ETSI) have included the descriptions and relationships of all the harmonised standards applicable for Europe in ETSI Technical Reports ETR010 and ETR076.

Usage EuroDomain, Carrier Telecommunication Services.

Security

- No specific standards for ISDN security are available and few are in development.
- The OSI standards developed to provide security mechanisms defined in IS 7498-2 should be utilised to the maximum extent possible.
- ISO/IEC 9594-8 provides a directory foundation upon which ISDN authentication may be built.
- A simple physical layer confidentiality protocol operating on any circuit switched ISDN channel octet stream using intra-channel security set-up signalling is required.
- Security support services should include key management, auditing and security fault recovery.
- Access control in public networks will require authentication protocols for performing identity based access control.
- Specific security mechanisms are the subject of standards development efforts of the JTC1/SC27.

2.13.2 LAN-LAN Interconnection Services

Functionality

Even though IP services are the preferred solution, a LAN-LAN Interconnection Service is available from the EuroDomain. This service is based on ATM and Frame Relay that provides interconnection of LANs regardless of the sub-net used (e.g. CSMA/CD, Token Ring or FDDI LANs), and with a high bandwidth. The currently emerging technology in this area is DSL (Digital Subscriber Line). Its advantage is that it works with copper wiring, which makes its implementation relatively easy. Support for DSL should be available before the end of 2001.

In the LAN case, the EuroGate should provide interconnection of LANs, regardless of the sub-net used. The EuroGate should particularly offer the services of routing, address conversion, filtering of traffic, and redirection. The service should be accessed via ISDN, or via a leased line.

Usage EuroDomain, Carrier Telecommunication Services.

Security

FDDI

- Fibre networks cannot be tapped into as copper-based networks can. FDDI adds to this basic security by forcing network nodes to announce their presence, which can help a network manager spot any unwanted intrusion.
- Security of the FDDI network relies heavily upon secure operation of the incurred management protocol. The standard chosen by the largest number of FDDI vendors is SNMP (Simple Network Management Protocol).

Frame Relay

- Simple CRC checking is sufficiently reliable at carrier services level, while message error recovery originated from e.g. lost frames at the frame handler congestion is left to the higher level protocols.
- To assure data confidentiality, sufficient data encryption at higher protocol layers and/or private network must be provided.
- Use a set of procedures and messages specified in ANSI T1.617 and ITU-T Q.933, defined to operate between a user device and a Frame Relay network, that provide status and outage notification for Frame Relay permanent virtual connections (PVCs).

ATM

- The scope of security for ATM networks includes aspects of network security, as well as administrative and operational security.
- The encryption used for ATM should be stream ciphers rather than block ciphers as the former can more easily be built to perform at high speed.
- An AAL-dependent cryptographic card needs to be embedded in the terminal equipment (a workstation for example). The alternative is to place a cryptographic hardware device outside the terminal equipment.
- Apply security services on a per channel basis.
- Protect the key distribution centre and the key distribution process.
- Use a wide word cryptographic processor and a cache for processor state information to ease key agility, i.e. the ability to access a range of key data at high speed.

Resynchronisation could be achieved via each cryptographic device sending an OAM cell at regular intervals on each virtual channel.

Reference information

DSL: The ITU-T recently pre-published the G.922 recommendation.

2.14 WAN Services

WAN services can be used over ISDN, FDDI, Frame Relay or ATM networks. The EuroDomain provides a Virtual private network service to interconnect LocalDomains.

The EuroDomain backbone network (i.e. TESTA II) has implemented Multi-Protocol Label Switching (MPLS), which is today a de facto standard and will evolve to support the Internet Engineering Task Force (IETF) Multi-Protocol Label Switching (MPLS) standard as soon as this is available (currently in Request for Comment, RFC process). MPLS combines the benefits of layer 3 routing with the advantages of layer 2 switching. In addition, MPLS is well suited for an integrated Internet Protocol (IP) and asynchronous transfer mode (ATM) environment.

The LocalDomain will access the European backbone on IP layer (layer three or networking layer) using RIPv2, Static-Routing, EBGP, or (in the near future) OSPF as routing protocol. Because of the nature of TESTA II, with multiple independent entities connected, special attention must be taken regarding the IP addressing and management.

2.14.1 IP Version 4 (IpV4)

Functionality

The rapid development of IP based networks leads to the definition of the next generation of IP protocol. The EuroDomain has to be ready to support this new version of the IP protocol.

IPv6 (Internet Protocol Version 6) is the latest level of the Internet Protocol (IP) and is now included as part of IP support in many products including the major computer. IPv6 has also been called "IPng" (IP Next Generation). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF). IPv6 was designed as an evolutionary set of improvements to the current IP Version 4. Network and intermediate with either IPv4 or IPv6 can handle formatted for either level of the Internet Protocol. Users and service providers can update to IPv6 independently without having to coordinate with each other.

In case of utilisation of Version 6 of the IP protocol, the EuroGate must provide a conversion mechanism that will allow a LocalDomain to use the EuroDomain IP version to communicate with other LocalDomains or with External Domains.

Usage EuroDomain, WAN Services.

Security

- Cryptography is a potent solution to many TCP/IP security issues such as eavesdropping or even message authentication.
- The TCP segment *checksum*, although it can serve as a one of the protection mechanisms, should NOT pose the only security solution since it can be easily confused with a reasonable probability because it is only 16 bits long.
- Reject pre-authorised connections if source routing information was present.
- A variation on this defence would be to analyse the source route and accept it if only trusted gateways were listed.
- A paranoid gateway – one that filters packets based on source or destination, like a firewall – has to block any form of host spoofing.
- Exterior gateways must be on the same network as the core gateways; thus, the intruder would need to subvert not just any host; but an existing gateway or host that is directly on the main net.
- The global routing table should not be modified in response to ICMP Redirect messages.
- Use of filtering and DMZ + firewall mechanisms is recommended. No routing protocol should be used in the DMZ.
- In an `Autonomous System' (AS*) WAN architecture usage of BGP 4.0 could be considered, see RFC1771. (The classic definition of an Autonomous System is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS, and using an exterior gateway protocol to route packets to other ASs.)
- Encapsulating Security Payload: RFC2406.

Reference information

- Technical Criteria for Choosing IP The Next Generation: RFC1726.
- Internet Protocol, Version 6 (IPv6) Specification: RFC2460.
- Transition Mechanisms for IPv6 Hosts and Routers: RFC1933.
- Routing Aspects Of IPv6 Transition: RFC2185.
- DNS Extensions to support IP version 6: RFC1886.
- Authentication Header: RFC2402.

Comments

- In future, EuroDomains may support VPN (via tunnelling protocols such as L2TP or PPTP) as a way of connecting to corporate information using the Internet rather than dial-in accounts. It is less expensive because companies who use VPN do not have to maintain extensive modem pools and accompanying telephone-numbers etc.
- Security is provided by means of a technique called tunnelling. Basically tunnelling creates a connection over the Internet as if it were a point to point connection. However, tunnelling is not yet applied in trans-European networks. A VPN using ‘tunnelling’ can be an alternative for other forms of point to point connections such as Frame Relay or leased lines.

2.15 Security Services and Secure Connections

Implementation issues of security have been described in Part I of these Guidelines. In addition to the security aspects that have been described in the individual service profiles, the security services described below are of relevance.

2.15.1 VPN (Virtual Private Network Services

Functionality

VPN is a technology that allows organisations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks.

PPTP, L2TP and Layer 2 Forwarding are among the most likely proposals as the basis for a new Internet Engineering Task Force standard. The protocols are used by ISPs to establish VPNs. With PPTP, which is an extension of the Internet's Point-to-Point Protocol, any user of a PC with PPP client support is able to use an independent service provider to connect securely to a server elsewhere in the user's company.

Usage Connectivity

Security

To assure reliable data transport use symmetric DES standardised by the US National Bureau of Standards or asymmetric RSA, a well-known public key.

Reference information

- RFC2401: Security Architecture for the Internet Protocol.
- RFC2406: IP Encapsulate Security Payload.
- Implementation of Virtual Private Network (VPNs) with IPSEC.

2.15.2 PKI (Public Key Infrastructure)

Functionality

The EuroDomain should provide services for a Public Key Infrastructure or “PKI”.

PKIs integrate digital certificates, public key cryptography (both combined in SSL), and certificate authorities into a security architecture. Nowadays Certificate Authorities can provide certificates with the accompanying public and private keys. The content of a certificate is described in ITU-T recommendation X.509 (8/97).

For the time being, certificates are issued by the IDA PKI Certification Authority. However, cross certification is sought by the Member States to set up their own national Certification Authorities (CAs), issuing certificates for their own Member State Administrations. A PKI should interact with these national CAs through cross-certification, and/or provide certification services where none exist.

A PKI could manage the generation of key pairs necessary for encryption, as well as the certificates used to provide confidence in the validity of these keys. The PKI solution should apply the following principles:

- provide an acceptable degree of confidence;
- take advantage of market products;
- be based on open standards;
- be suitable for an international environment;
- satisfy technical and legal constraints;

- recognise national responsibilities and the principle of decentralised responsibility;
- be user friendly.

A uniform PKI allows cost-effective security to be provided to a full range of applications, thus avoiding the need to support different security architectures for each sector application. In order to use a PKI on a European-wide scale, the following issues must be resolved:

- interoperability of the PKI with other certification authorities and the possibility to recognise certificates provided by such authorities;
- ability to validate the status of the certificate (e.g. CRLs, OSCP, etc.);
- capability to carry key management traffic over a variety of standard transport protocols (e.g. LDAP, Internet Mail, X.400, HTTP);
- Capability to use the European wide EuroDomain backbone transport for certificates and key management traffic.

Usage EuroDomain, Security Services.

Reference information

- PKICUG project documents

2.15.3 IPSec

Functionality

IPSec allows authenticated and encrypted communication between routers, between firewalls, and between routers and firewalls. IPSec provides a strong foundation for implementing security at the IP layer. IPSec compliant products provide interoperability and a minimum standard of security. Because the framework of IPSec is broken into components new algorithms and key exchange protocols can be implemented and easily integrated into an existing IPSec compliant environment.

IPSec was designed to define a framework and set of mechanisms to protect the confidentiality, integrity, and provide authentication of the data passed over IP networks. These mechanisms work at the IP layer and are designed to be algorithm independent. This means that even though the IPSec standard defines default algorithms, the definition and structure of the mechanisms used allow additional algorithms to be easily added in.

Security measures

IPSec consists of three components are the Authentication Header (AH) Protocol, the Encapsulating Secure Payload (ESP) Protocol, and Key Management.

The IP Authentication Header (AH) is designed to provide strong authentication and integrity for IP datagrams. With asymmetric digital signal algorithms, such as RSA, the AH can provide non-repudiation.

The IP Encapsulated Secure Payload (ESP) is designed to provide confidentiality and integrity for IP datagrams. Depending on the algorithm used ESP may also provide authentication. ESP can be implemented in two different ways, tunnel mode and transport mode.

The key management serves as a foundation for the security provided, and the AH and ESP protocols define the structure that provides authentication, confidentiality, and integrity of the data.

Usage EuroDomain, EuroGate, Security Services.

2.15.4 Java Security

Functionality

When centralised, transactional services are implemented on a common LocalDomain using the J2EE platform, embedded Java security will need to be considered in application design. The Java security approach addresses the following problem domains:

- code-centric access control approach: offering a safe environment in which to run potentially untrusted code downloaded from the network onto a client. With the latest release of the Java Platform, fine-grained access controls can be placed upon critical resources with regard to the identity of the running applets and applications, which are distinguished by where the code came from and who signed it;
- enterprise application, user-centric access control, to deal with different users, either concurrently or sequentially, and grant these users different privileges based on their identities. The Java Authentication and Authorisation Service (JAAS) is designed to provide a framework and standard programming interface for authenticating users and for assigning privileges;
- cross-application security, to implement secure exchange of messages between communicating applications.

Together with Java 2, an application can provide code-centric access control, user-centric access control, or a combination of both.

JAAS can be used for two purposes:

- for authentication of users, to reliably and securely determine who is currently executing Java code, and
- for authorisation of users to ensure they have the access control rights (permissions) required to perform security-sensitive operations.

Security measures

Java GSS-API is used for securely exchanging messages between communicating applications. The Java GSS-API contains the Java bindings for the Generic Security Services Application Program Interface (GSS-API) defined in RFC2853. GSS-API offers application programmers uniform access to security services atop a variety of underlying security mechanisms.

Because in the IDA architecture inter-Domain communications are to be implemented over loosely coupled services across the LocalDomain firewalls, this API is ONLY relevant when distributed systems are implemented inside a LocalDomain providing a centralised service.

The relationship between JAAS and Java GSS-API is that JAAS authentication is typically performed prior to secure communication using Java GSS-API. Thus JAAS and Java GSS-API are related and often used together.

However, it is possible for applications to use JAAS without Java GSS-API, and it is also possible to use Java GSS-API without JAAS. Furthermore, JAAS itself can be used simply for authentication or for both authentication and authorisation.

2.15.5 Cryptography and Authentication Services

Functionality

SSH: (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is intended as a replacement for rlogin, rsh, srcp, and rdist. Because of security problems with these programs their use is not recommended. SSH is being standardised in an IETF Security Area secsh working group.

Current Internet-Drafts

- SSH Protocol Architecture
- SSH Transport Layer Protocol
- SSH Authentication Protocol
- SSH Connection Protocol

Security measures

- Use Public Key – Private Key encryption algorithm for data confidentiality.
- Use X.509 based certification systems.
- Use smart cards or one-time password mechanisms for authentication.
- Use PEM [22][23][24][25], MOSS[26], PGP[27] or S/MIME

Usage EuroDomain, EuroGate, Security Services.

2.15.6 Firewalls

Functionality

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network by determining which inside services may be accessed from the outside, which outsiders are permitted access to the permitted inside services, and which outside services may be accessed by insiders. A firewall is installed in a specially designated computer separate from the rest of the network so that no incoming request can reach private network resources directly. A typical firewall is composed of one or more of the following building blocks:

1) **Packet-filtering router** - The router screens each datagram to determine whether it matches one of its packet-filtering rules based on the IP packet header data (i.e IP source address, the IP destination address, the encapsulated protocol -TCP, UDP, ICMP, or IP Tunnel, the TCP/UDP source port, the TCP/UDP destination port, the incoming interface of the packet, and the outgoing interface of the packet, etc.) The packet-filtering rules also enable a router to permit or deny traffic based on the service listeners residing on designated TCP/UDP port numbers. (e.g. a RDBMS server may listen for incoming connections on TCP port 1431.) The router may be configured to deny all packets that contain a designated TCP destination port value to restrict a service’s incoming connections to certain hosts.

2) **Application-level gateway** (or proxy server) - The Proxy Server works as a relay between two networks, breaking the connection between the two. All input is forwarded from a different port, closing a straight path between two networks and preventing intruders from obtaining internal addresses and details of a private network. (Using Network Address Translation, NAT, proxy services enable a network to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic.) While packet-filtering simply allows managing the flow of Internet services through the firewall, a proxy service provides much stricter security because it involves special-purpose code that is installed on the gateway for each application: if the proxy code is not installed for a particular application, the service is not supported and cannot be forwarded across the firewall. Because the system hosting the proxies is extremely secure (i.e. it only runs a limited set of proxy applications and is based, in general, on a secure firewall-specific Unix version) this solution is called “bastion host”.

3) **Stateful inspection** - A firewall can track a transaction in order to verify that the destination of an inbound packet matches the source of a previous outbound request. Generally, it can examine multiple layers of the protocol stack, including MAC-level, so blocking can be performed at any layer or depth. Unlike application level gateways, stateful inspection uses business rules defined by the user and therefore does not rely on predefined application information. Because specific applications cannot be recognised, the same rules apply to different applications. Stateful inspection takes less processing power than application level analysis.

4) **Circuit-level gateway** – This mechanism relays TCP connections by simply copying bytes back and forth between the inside connection and the outside connection, without performing any additional packet processing or filtering. Yet it is very effective, because the connection appears to originate from the firewall system, it conceals information about the protected network.

5) **Demilitarised zone network** – A firewall system combining the packet-filtering routers-based solution and a bastion host-based solution. This firewall solution supports both network and application-layer security by defining a "demilitarised zone" (DMZ) network as a small, isolated network between the two networks to be connected, facing them through packet-filtering routers. The network administrator places the bastion host, information servers, modem pools, and other public servers on the DMZ network. Systems on the Internet and systems on the private network can access only a limited number of systems on the DMZ network, but the direct transmission of traffic across the DMZ network is prohibited. This solution is most secure, because an intruder must crack three separate devices (without detection) to infiltrate the private network: the outside router, the bastion host, and the inside router.

6) **Content Inspecting** – Since a firewall oversees all network traffic, it may be seen as the appropriate location for software that performs content inspection against viruses. A number of firewall products embed content inspecting against viruses in SMTP, HTTP and FTP traffic in a unique security management environment. Virus scanning occurs at the server, so it is transparent to end-users. The tools also detect and block potentially harmful ActiveX and Java code. Administrators are enabled to create rules for blocking messages containing words or phrases associated with e-mail carrying virus-infected attachments. In addition, administrators can also choose to block file attachments containing certain macros as a preventative measure while waiting for an updated virus pattern file.

For mobile users, firewalls allow remote access to the private network by the use of secure log-on procedures and authentication certificates.

Commercial firewall products are shipped in many variants. In general, common features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall.

Usage: EuroGate

Whatever network services are chosen to build the EuroDomain, a proxy server needs to be set up to:

- Perform network address translation (NAT). NAT (an IETF standard enabling a LocalDomain to use one set of IP addresses for internal traffic and a second set of addresses for external traffic) channels all user requests to the EuroDomain and returns responses to the appropriate users, performing the requisite address conversion back and forth. NAT is necessary to set up an addressing schema for internetworking that does not affect address schemas used inside LocalDomains.
- Build firewall protection, that must be especially thorough if the EuroDomain services are provided by the Internet.

Implement a firewall to protect the LocalDomain against unauthorised access from the Internet (e.g. if a public Web server is running in the LocalDomain, a firewall is needed to separate it from the internal network) and to keep internal network segments secure. Use a firewall to restrict traffic from LocalDomain to EuroDomain. In particular:

- Implement a dual-home gateway (router with access lists and implementation of Network Address Translation (NAT) to filter out all network traffic to the EuroDomain other than that originating from LocalDomains.
- Implement a screening router with access lists, NAT and a bastion host to restrict the network traffic to the TESTA IP backbone only in order to connect to another remote LocalDomain.
- Implement a DMZ network to restrict network traffic, control identity of any users, and protect confidentiality of any information from the outside world when connecting to the Internet.

2.15.7 Virus Protection and E-mail Attack Countermeasures

Functionality

Viruses present risks including system disruption, unauthorised access to computer systems, misuse of telecommunications facilities, computer-based fraud, and demonstration of the intelligence of their authors. Threats can be posed by:

- A *virus* is a self-replicating program that can infect other programs, either modifying them directly or by modifying the environment in which they operate. When an infected file is executed, this will cause a virus code within the program to be run.
- A *worm* is a program, which attacks computers that are connected by a network and spreads by sending a copy of itself through the network to infect another machines.
- A *Trojan horse* is a program that pretends to be something it is not. Often it is a program that has the same name as a legitimate one, but only to allure an unaware user and when executed, may perform an unexpected behaviour.
- An *e-mail bomb* is a software equivalent to a letter bomb. The bomb may explode either at the time the letter is being read, for example reserving a major portion of system resources, or later on, especially when run an e-mail conveyed attachment, which in turn contains a virus, often a Trojan horse.

To protect against viruses and to cure the affected systems there is a number of commercially or shareware available programs known also as *antiviral software*.

Protection measures

Use the best, up-to-date anti-virus program to check every attachment, especially executable files or other active objects, before they are used in any way. Open e-mail messages using a reliable and stable e-mail-assistant program that is capable of handling all resources needed to open a given e-mail and store its potential attachment. Limit the size of attachments.

Usage EuroDomain, EuroGate, Security Services.

2.15.8 S/MIME (Secure/Multipurpose Internet Mail Extensions)

Functionality

S/MIME is a specification for secure electronic mail and was designed to add security to e-mail messages in MIME format. The security services offered are authentication (using digital signatures) and privacy (using encryption). S/MIME was designed to be interoperable, so that any two packages that implement S/MIME can communicate securely.

S/MIME uses a hybrid approach to providing security, often referred to as a “digital envelope”. The bulk message encryption is done with a symmetric cipher, and a public-key algorithm is used for key exchange. A public-key algorithm is also used for digital signatures. S/MIME recommends three symmetric algorithms: DES, Triple-DES, and RC2. The adjustable key size of the RC2 algorithm makes it especially useful for applications intended for export outside the U.S. RSA is the required public-key algorithm. S/MIME also supports digital certificates. The X.509 format is used due to its wide acceptance as the standard for digital certificates.

Usage EuroDomain, EuroGate, Security Services.

2.16 Open Source Software

Open source software is software for which the source code is distributed along with the executable program, and which includes a license allowing anyone to modify and redistribute the software. Actual licenses for OSS vary between different companies and development projects, but they have certain characteristics in common.

The Open Source Initiative, a group of developers who disseminate information on the benefits of open source, has posted on its web site a "meta-definition" of basic conditions which they feel should be included in an OSS license. These conditions include:

- Allowing free redistribution of the software without royalties or other fees to the author.
- Requiring that source code be distributed with the software or otherwise made available for no more than the cost of distribution.
- Allowing anyone to modify the software or derive other software from it, and to redistribute the modified software under the same license terms.

Any software which is distributed under a license which conforms to these requirements is open source software, according to the Open Source Initiative. License models include:

- The GNU General Public License (GPL);
- The Berkeley Software Distribution License (BSD);
- The Mozilla Public License (MPL).

The complete list of licenses approved by OSI (Open Software Initiative) can be found at:

www.opensource.org/licenses/index.html

The IDA website (http://www.ispo.cec.be/ida) contains a report of a study into the use of open source software in the public sector. The report consists of:

- an assessment of availability and potential of OSS-based solutions;
- a selection of approx. 100 typical OSS solutions (out of several thousands of OSS projects);
- a study into the use/non-use of OSS in their public sectors; how OSS may be used and distributed according their licenses, and how the legal and commercial aspects may impact public procurement objectives, transparency and non-discrimination.

Examples of Open Source Software that have been applied successfully include:

- Linux, that runs on approx. the world servers;
- Apache, which runs over 60% of the world's web servers;
- Perl, which is the engine behind most of the `live content' on the World Wide Web;
- BIND, the software that provides the DNS (domain name service) for the entire Internet;
- Sendmail, the most important and widely used email transport software on the Internet.

Some solutions, such as DNS and Sendmail, have become `solution killers', not only because they are capable and robust, but also because no commercial competition has been sufficiently successful in replacing them.

Once limited to “small budget environments” such as educational institutions, Open Source Software is now gaining momentum in other sectors. The generalisation of Open Source and the success of the above-mentionned products have now dissipated the fear of uncertainty that used to be a common attitude.

3 Best Practice Examples

3.1 Introduction

The following Best Practice Examples demonstrate how the IDA Architecture and its generic services and common tools have been put into practice.

Each Best Practice Example text has the following structure:
- introduction, giving a general description and the objectives of the project;
- technical approach;
- standards and technologies used in the project approach.

3.2 EIONET

3.2.1 Introduction

EIONET is a collaborative network of the European Environment Agency and its Member Countries, connecting National Focal Points in the EU and accession countries, European Topic Centres, National Reference Centres, and Main Component Elements. These organisations jointly provide the information that is used for making decisions for improving the state of environment in Europe and making EU policies more effective. EIONET is both a network of organisations and an electronic network (e-EIONET).

The legal basis for EIONET is the European Environment Agency's (EEA) objective of ensuring the supply of objective, reliable and comprehensive information at a European level and of ensuring that the public is properly informed about the state of the environment. Moreover, the EEA supports the development of Environmental Assessment methodologies and best practices, and assists the diffusion of information on the results of relevant environmental research.

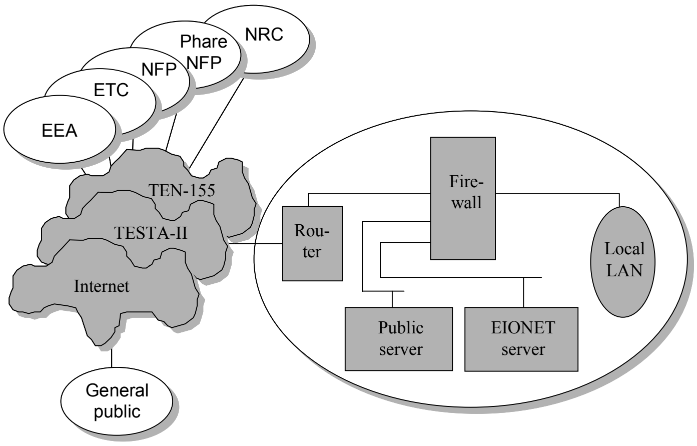
The objective for the EEA/EIONET is to achieve a situation where a fully operational environmental indicator system is available for European countries supported by decentralised - but stratified - data flows from country level to European level. All information production for European environmental reporting will in future be arranged to flow through an unbroken electronic value chain so that manual work can be minimised and incompatibilities avoided, duplicate work eliminated, and data and information stored in proper places in usable form, also for public access.

In future, e-EIONET will contain in its directories and information repositories sufficient knowledge for the organisational EIONET to seamlessly support users in their functional duties. This will be achieved through interoperable information systems where users voluntarily use e-EIONET to contribute to the maintenance and storage of the reusable knowledge.

3.2.2 Technical approach

Network architecture

Internet remains the carrier of choice for the e-EIONET because of the large number of organisations (hundreds) and enterprises that need access. However, the existing backbones of TEN-155 and the IDA generic service TESTA II will be used where feasible. Those nodes that already are in these high-speed backbones enjoy faster connections, but routing shall be possible between all the nodes.



Network	Use of existing connections, i.e. TESTA II or TEN-155.
Security	IDA's generic services and common tools, i.e. PKICUG where applicable.
EIONET servers	Current EIONET servers; in future, Linux-based next generation server.
Network Management Centre	Usage statistics, monitoring of workflow, replication of content between nodes.

Group collaboration and portal development

EIONET adopted CIRCA, which has been enhanced at EIONET for its e-mail management and with portal interfaces. This customisation is gradually growing, and the extended product that is integrated across all sites is known as the EIONET CIRCLE.

Group collaboration and portal integration	• CIRCA engine as a generic service for web, directory, newsgroups, search, e-mail. • CIRCA common tools such as the library tool, meetings and newsgroups, workflow and portal management tools. • Customised CIRCA functions for roles, organisational info, and dynamic mailing lists
Application packaging and personalisation interfaces	• CIRCA groupware. • Electronic workplace, My-EIONET. • Corporate portal.
Developer interfaces for group collaboration and portal integration	• Perl, Python, Java, and C code. • Zope application server and the EIONET Portal Toolkit. • Open Source Policy, supported by Mozilla Public License. • XML DTDs for data interchange. • RSS for site descriptions.

Data management and data flows

Data definition tool for data modelling and maintenance of data dictionary	• Build on results from TERESA project. • US EPA electronic data registry tools. • Public domain metadata tool. • CASE tools.
Data storage / data warehousing	• Will be developed from open source components from MySQL community, e.g. the Generic Information Server Toolkit (GIST) of the JRC.
Data collection, validation and exchange	• STATEL for data collection. • DEM (Data Exchange Modules) tools developed as Web forms, e.g. ASCII files or XML documents.
Data visualisation for analysis and browsing content	• TERESA. • EEA's NATLAN system.

Portal development

Generic services underlying portals	• Zope application server from public domain, which allows dynamic content provision, delegation of authority in content management, XML-support, MySQL database integration, and has a solid approach to modularity and open source. • US EPA electronic data registry tools. • Public domain metadata tool. • CASE tools.
Common tools for portals	• Portal toolkit using Zope. • XML. • RSS (Rich Site Summaries).
Portal applications and user interfaces	• Existing Internet, Extranet and Intranet services as a basis. • The push-technology search engine that was created under the APPLIC PUSH project will be integrated with the EIONET portal. This engine collects meta-information on new documents on participating EIONET sites each night.

3.2.3 Overview of service components used by EIONET

EIONET makes use of the following generic services and service components:

- TESTA
- PKICUG
- CIRCA
- Networking protocols
- Middleware
- Directory access protocol
- J2EE model

3.3 EURES

3.3.1 Introduction

EURES provides a trans-European telematic network linking employment services across Europe. EURES maintains a comprehensive database of job vacancies, as well as information on living and working conditions in the different Member States. Some 500 Euro-advisors provide local advice to job seekers and employers on opportunities and resources available abroad.

The legal basis for EURES is found in Article 4 of the Council Decision 1719/1999/EC: to implement networks in the field of policies related to the free movement of persons. Moreover, the Maastricht treaty provides European citizens with the freedom to move between Member States, without bureaucratic restraints. EURES's task is to enable citizens to easily identify employment opportunities in other Member States and to provide them with the practical advice needed when exercising their freedom of movement.

EURES has implemented a private IP telecommunications network (TESTA) as well as a client/server application. Employment data are now stored in a central database, which then distributes this data to the databases of its integrated partners, which include France, Germany, Austria, Norway, Finland, The Netherlands, two regional partners in Belgium, one regional partner in Italy and APEC in France.

EURES's network runs over the TESTA VPN. In addition, the EURES database is directly accessible to citizens via the Internet.

EURES is coordinated by DG Employment and Social Affairs. Currently, 22 employment services in 15 Member States and 2 EFTA countries are active partners in the EURES network.

3.3.2 Technical approach

EURES is a network of national databases and a European database, linked together by a private pan-European IP telecommunications network (TESTA). The national relational databases run under UNIX systems.

The 500 Euro-advisors access the EURES database using a PC client/server application, using middleware over UDP/IP.

Employment data is exchanged between national offices using FTP. Transcoding and translations of data are performed on both the national systems and the EURES system according to bilateral agreements.

The network will migrate to TESTA II. The Internet services will be expanded to all European job vacancies, partner sites, and information and CV databases.

3.3.3 Overview of service components used by EURES

EURES makes use of the following generic services and service components:

- TESTA
- FTP

3.4 EudraNet

3.4.1 Introduction

The EudraNet network links the European Commission DG3, the European Agency for the Evaluation of Medicinal Products (EMEA) and the competent Member State authorities (MSAs) for medicinal products for human and veterinary use. It is used for the exchange of regulatory and scientific information and for the exchange of pharmacovigilance information. It also hosts a common database with procedures for marketing authorisation through Mutual Recognition and a database of Safety reports.

At present the users involved are 27 MSAs, EMEA, the JRC (Joint Research Centre of the Commission) and DG3 of the Commission. There are around 700 e-mail identities/addresses created in EudraNet applicable to functional domains and working groups. There are around 60 users registered for the common databases. In the future, the network may be extended to the EEA, and Central and Eastern European Countries. There is an identified need to facilitate the electronic communication between the regulators in EudraNet and more than 200 companies in the pharmaceutical industry.

EudraNet is used to exchange highly confidential regulatory and scientific information between the network partners. There is a need for confidentiality that will be resolved by the services of a PKI (Private Key Infrastructure) at European level. EudraNet is a good example of the IDA EuroDomain model and therefore should provide applications with optimal inter-operable and scalable services.

The legal basis for EudraNet is Council Regulation 2309/93, which states that a data processing network must be set up for the rapid transmission of data between the competent Community authorities in the event of an alert relating to faulty manufacture, serious adverse reactions and other pharmacovigilance data regarding medicinal products marketed in the Community.

3.4.2 Technical approach

EudraNet provides the following technical services:

- Network services;
- DNS and Routing Services;
- Message Handling Services;
- Web Services.

Network services

EudraNet is designed as a managed IP private network. It follows the IDA architecture and is implemented through TESTA.

DNS and Routing Services

Addressing and routing of connections between EudraNet hosts and workstations are provided by the EudraNet DNS server. EudraNet relies on the eudra.org domain that is part of the Internet DNS system via the JANET Internet Service Provider. This domain is subdivided into various sub-domains, each of which contains a given number of IP addresses according to the EudraNet IP policy.

One sub-domain includes those hosts of EudraNet that can be reached from networks outside EudraNet. The other sub-domains have a set of IP addresses not reachable from the Internet DNS system and therefore inaccessible for the Internet users. EudraNet provides internal DNS services to those private domains unreachable via the Internet.

The DNS service includes a number of firewalls (proxies) that act as gateways between external and internal EudraNet domains. These gateways protect the internal domains while permitting internal hosts to communicate transparently with Internet external hosts.

Message Handling Services

The EudraNet Message Handling System includes e-mail and directory services based on SMTP and LDAP respectively.

Web Services
EudraNet provides a web page that is only accessible by the network partners. This web page contains a repository of documents exchanged between the EC, the EMEA and the Member States, and links to common databases.

The EudraNet web also provides tools to configure e-mail accounts, information about the cases processed by the helpdesk, and a diagram showing the status of network connectivity.

3.4.3 Overview of service components used by EudraNet

EudraNet makes use of the following generic services and service components:

- TESTA
- PKICUG
- CIRCA
- Networking protocols
- Message Handling
- Directory access protocol

3.5 Communication and Management of Official Documents

3.5.1 Introduction

CMOD aims at the modernisation of the exchange of official documents between the institutions so as to improve the efficiency of the decision making processes. To offer this support CDOM will set up the necessary telematic links between the Commission, European Parliament, other European institutions and the Council. Moreover, in support of multilingualism in inter-institutional information exchanges, CDOMN supports the translation workflow management, translation support tools, sharing and exchanging of multilingual resources, and organisation of common access to terminology databases.

CMOD's objectives are as follows.

- Implementation of reliable document flows between the institutions, replacing mostly the current paper-based flows and improving the efficiency of inter-institutional procedures.
- Definition of reliable and stable document formats, and implementation of the appropriate mechanisms guaranteeing their authenticity
- Implementation of efficient document delivery methods, making them immediately accessible to those interested (ministers. MEPs, agencies, etc.), wherever they are located in Europe.
- Setting up consolidated inter-institutional procedure management systems.
- Increased transparency of Community activities and acceleration of the publication process.

3.5.2 Technical approach

- Migrate to TESTA
- Start using XML for meta-information and for operational document structuring
- Implement CIRCA for the comitology sub-project

Greffe 2000 and Legiswrite sub-project	• TESTA/PKICUG. • XML for meta-information. • Implement web-based technologies.
Parliamentary Questions	• XML for document exchange. • Electronic transmission of preliminary versions of parliamentary questions. • Web-based approach for document flows.
Inter-institutional procedures follow-up	• Exchange of structured data between the Parliaments's system TECOM and the Commission's PERSEE-SG-Vista databases. • XML as format of transmission forms accompanying official documents.
Comitology	• CIRCA for notification of Parliament. • XML.
Inter-institutional directories	• Interconnected directories to support e-mail and workflow technologies. • UML for inter-institutional exchanges.
Trusted exchanges of official documents	• Security solutions from IDA horizontal projects, i.e. digital signature, trusted certification centre, checksum, security standards, open standards for exchange of documents (XML/ICE, NewsML, ParLML, workflow processes.
Inter-institutional access to translation memories	• EURAMIS system (an e-mail based client/server application developed within the Commission) for access to language applications.
Metadata and link management	• Standardisation of metadata.

3.5.3 Overview of service components used by CMOD

CMOD makes use of the following generic services and service components:

- TESTA
- PKICUG
- CIRCA
- Middleware