ARCHITECTURE GUIDELINES

For Trans-European Telematics Networks for Administrations

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

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 6.1 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 Executive Summary

1.1 Mission Statement

These Guidelines describe an architecture agreed upon by the IDA (Interchange of Data between Administrations: a European Community Programme) community that enables trans-European networks to interoperate, and thus allowing Public Administrations in Europe to interchange data. Since this architecture is of crucial importance for the exchange of data and the collaboration between Member States and Institutions, the European Council continuously pays considerable attention to its development, implementation and operation. In 1999, the Council addressed the Architecture as well as its Guidelines in its Interoperability Decision[1].

The Interoperability Decision mandates the IDA programme of the European Community to provide a stable foundation that must support Trans-European network implementation and deployment, in order to achieve interoperability and economies via reusability of components and practices.

The architecture described in these Guidelines constitutes this foundation. It consists of a coherent application model and a set of pre-built, generic services and tools for enabling development, deployment and management of business applications.

It is the responsibility of the IDA Programme to design and continuously update this architecture, ensuring correspondence with user requirements and emerging technologies. In addition, the architecture must support and stimulate the use of generic services and common tools that are being developed in projects.

The Architecture guidelines are one of these generic services. The guidelines are designed to support the Interoperability Decision goals, by providing:

- architectural principles to ensure a coherent, generic services-based approach to developing Trans-European telematics networks;
- guidance on how to use common tools as soon as these are made available by the IDA programme to the EU user community.

It is the role of the Guidelines to reflect the vision of the IDA programme on the telematics platform that it offers to its user community by means of the architecture described here. As the requirements of the community change and evolve, along with the constant emergence of new technologies, the architecture and its guidelines must change. Moreover, the architecture and its guidelines must constantly adopt and promote generic services and common tools.

The role of these guidelines must, therefore, be that of a dynamic communication instrument that changes along with the constantly evolving architecture and its components. This role can only be sustained and enhanced if the guidelines are updated on a regular basis. Ideally, the guidelines are updated each time components of the architecture change or as new services and tools become available. In this respect, the current version offers a large amount of new information on technologies in the field of middleware, a field that will be extended even further in the next version of these guidelines.

As a central platform and publishing tool, the Guidelines can offer access to a variety of information sources and documents that are related to the architecture. In its electronic HTML and PDF formats, these references are facilitated by hyperlinks.

[1] Decision 1720/1999/EC of the European Parliament and Council adopting a series of actions and measures in order to ensure interoperability and access to trans-European networks for the electronic interchange of data between administrations (IDA), adopted on the 12 July 1999. OJ L203 of 3.8.1999.

1.2 Audience

The guidelines address two main audiences:

- those responsible for planning, design and procurement tasks relating to trans-European horizontal actions and measures, in particular generic services and common tools;
- those responsible for the development of specific, sectoral projects for the interchange of data between administrations.

The former group may use this document as the basis for the development of specific, detailed requirements for the provision of the necessary Trans-European network services supporting IDA projects.

The latter group may use the architecture concepts and associated references when defining their specific project architecture, and integrate into the projects those parts of the technical specifications relevant to them.

1.3 Scope

This document describes concepts and references to be used for the implementation of a Trans-European Service for telematics built on a well-defined common architecture. This architecture is the base for a Trans-European infrastructure that must enable easy and reliable interchange of data and ensure optimum inter-operability of networks and electronic data transmission between European Institutions, European Agencies, and Administrations in Member states.

Adherence to these concepts and recommendations will improve inter-operability between local telematics systems and consequently reduce implementation costs and allow replication of achievements.

1.4 Benefits

The direct benefits of having such common concepts and references are intended to be:

- improved inter-operability between the IT and networks systems of business partners;
- clear delineation between the responsibilities of the business partners in terms of funding, operation, and management;
- continued autonomy of the business partners to select the architecture for their IT solutions, and to develop it, without being dependent on the architecture at the community level.
- continued autonomy of business partners to select the service provider who can implement the concepts and components that comply with the Architecture Guidelines, thus providing controlled, secured, managed, transparent and easy access to the common Trans-European Services.

The Architecture Guidelines should be used as reference material whenever procuring or implementing services that do access the Trans-European Services, or as a technical framework for the achievement of generic services, i.e. telecommunication services made available to any kind of application.

Building IDA generic services on a common architecture will bring:

- reduced total costs through reusability and economy of scale;
- shorter time to implement new projects;
- improved manageability of projects and of the implemented solutions;
- setting a clear migration path for existing, heterogeneous projects;
- leaving Administrations to concentrate on their core business: applications.

1.5 Document Structure

This document is divided into two sections, section I – User Requirements and Implementation Principles – and section II – Implementation Approach and Guidance. Section I provides general information on architectural principles to be enforced in real-life projects. It moves on from general business requirements to architectural principles on how to meet such requirements.

Section II provides strategies for implementing the architecture and guidance that starts from the requirements described in section I and that helps to identify solution outlines and the services that offer these solutions.

The Annexes contain reference technical specifications for candidate technology (i.e. either generic services or, when available, common tools) to meet the requirements, as well as a number of Best Practice Examples of projects that have implemented components of the architecture covered by these guidelines.

1.6 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.

1.7 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.

Section I

User Requirements and Implementation Principles

2 Survey of User Requirements

2.1 Introduction

To ensure the relevance of the architecture and the extent to which its services address the needs of the user community, it is of crucial importance to:

- investigate user requirements;
- convey these to all parties involved (users, procurers, developers, managers, etc.);
- manage these requirements;
- regularly perform audits to see that requirements are being met by the services being provided.

This chapter reflects a current analysis of user requirements. Chapter 5 provides a roadmap that starts from the requirements described here and shows the path to solution outlines and the services that offer these solutions.

2.2 Fundamental Requirements

The primary principles enforced by the architecture guidelines are decentralised responsibility and interoperability. Decentralised responsibility involves the capability for the business partners concerned with trans-European networks to organise the data processing systems and networks in a way best suited to their practices (i.e. technological approach, legal framework, principles of management, etc.) Interoperability is achieved via a common architecture at a Community level for the interchange of data between heterogeneous systems that defines Community-wide services compatible with a common model.

The direct benefits of decentralised responsibility support are:

- autonomy of the business partners to select the architecture of their IT solutions, and to develop it, without being dependent on the architecture at the community level;
- autonomy of business partners to select the service provider that will be able to implement the concepts and components complying with the Guidelines to enable controlled, managed, transparent and easy access to the common Trans-European Infrastructure.

Interoperability is achieved by selecting a common set of architecture specifications and generic services that expose interfaces and rules at all levels (i.e. technical, managerial and operational) for the business partners' networks to use application services developed on top of them. In addition, a number of common tools are made available by IDA for immediate use in trans-European network implementation.

This approach is expected to bring economy of scale and shorter implementation time via reusability of components, while improving project manageability on account of a consistent approach across multiple projects. Ultimately, business partners are increasingly less involved in design concerns and concentrate on the very business at hand.

2.3 Generic Business Requirements

Trans-European networks are established to support business processes that involve independent partner organisations. Business types and requirements are wide ranging, yet common business requirements can be identified and classified based on the substantive commonality of the underlying processes.

Relevant requirements are those of organisations in the Member States (MSAs), EU agencies and Commission Services that are either mandated by law or simply encouraged to collaborate over common interest business.

Most such business processes have a regulatory origin. They are based on EU legislation placing upon MSAs and EU institutions an obligation to exchange particular types of formal documents (e.g. notifications), or to make information available to designated parties. In such cases the related applications may have a sensitive nature. In other cases, applications are simply put in place to allow smooth communication between parties involved. Some current trans-European projects are aimed to provide work groups with the means to perform collaborative work interactively.

The generic requirements can be classified as follows.

Users who need to exchange, share and manage information:

- inside the user community with trusted partners, with an agreed level of security and confidentiality and with diverse formats agreed for document management inside the community;
- outside the user community with external non-trusted partners, with a maximum of openness in the sense that access to protected resources residing inside the user community is controlled and does not pose security threats and with offered formats to the outside.

Users who need to search, query, access and optionally retrieve information, wherever this information is located:

- inside the user community, specifically for dedicated business and protected information generated by the user community;
- outside the user community, for information available in the external world to that user community (it could be either the public, or another user community or both).

The above mentioned requirements are addressed by the following five information processes:

- data exchange
- data collection
- data dissemination
- data sharing
- alert

Data exchange involves relevant data being mutually exchanged between two users/applications. This model is frequently used, especially when legislation attaches particular importance to the exchange itself (i.e. formal notifications) but also because it preserves independence of the counterparts that only need to agree upon a business exchange format and to set up a translation/conversion process on their existing application systems.

Data collection means that relevant data is gathered from distributed sources into a European data collector (hosted e.g. by Commission, Agencies, etc.). This model is suitable when a central organisation is responsible for, or is simply willing to provide, support or coordination services.

Data dissemination means that relevant data is centrally stored; data is accessed from distributed points by query/answer processes. This model provides both a counterpart to model [b], but is also increasingly used as an alternative to data exchange [a] using interactive means (partner systems expose light client-based interface to counterparts e.g. XML or Java-based).

Data sharing refers to processes in which data need to be shared in order to allow several departments or persons to collaborate in the activities to be performed on the data.

Alert refers to a type of communication, generally based on a kind of "push" mechanism, that must be triggered upon a certain event and reach its recipient within a defined time scale, and involves a common context between users (security, authentication, etc). Not to be mistaken for acknowledgement (that is more of a service process, applying to other communication forms.)

Furthermore, the following business issues are relevant in this context:

Timeliness, which refers to the period within which a required result must have been obtained or an action must have been performed. This marks the difference between a requirement for data exchange/collection and data sharing.

Legal issues, e.g. the obligation to deliver particular data influencing the type of contents to be handled and the communication mechanism chosen.

2.4 Security Requirements

For most applications, the use of the network depends on the assured security level and functions. These functions should be as transparent as possible to the user and involve a minimum of effort, and at the same time, provide an agreed level of security.

Security aspects that need consideration for individual projects are:

Confidentiality: The user must be assured that the services provided will not expose the data kept or transported to any party, who is not authorised to see it.

Availability: Constant availability of the services may be crucial to the end user. For this reason, the operator must guarantee the agreed availability, and take all necessary steps to maintain it.

Consistency, integrity: The network provider must guarantee that the data kept or transported is not changed in any way, in order to preserve the integrity of the information content.

Authentication, access control: When exchanging information between end users and systems it may be necessary to supplement the data exchange with a procedure to verify the identity of the user and/or the system, and to allow/deny access. This involves an authentication procedure that can take place at two different levels,

- at network level (address exclusion range, closed user groups mechanisms);
- at application or operating system level (access by user identification, accompanied by some token and/or certificate).

Non-repudiation: For some types of information exchange, it may be of significance (formally, legally, or commercially) that neither the sender nor the receiver can repudiate the fact that the information was sent and received.

Public domain information requires protection against unauthorised or accidental modification of data that would just cause disruption to the service. Normally prevailing security measures are sufficient guarantee in this respect.

Confidential information calls for protection against the risk of disclosure to non-authorised persons on a “need-to-know” basis. In this case, the underlying business process only allows designated people within the partner organisations to view or modify the information, based on their role in the business process. Such an authorisation schema is to be enforced by means of profile-based information security mechanisms.

Sensitive information involves an even stricter authorisation schema, where designated individuals only are allowed to view or change the information. System in this area may require strong security mechanisms based on encryption and digital signature.

Across all security requirement classes, ***information system integrity*** is always implied to prevent damage to resources inside systems and networks hosting the service.

2.5 Implementation Requirements

A number of value added services have been identified as necessary to facilitate the communication services or achieve the necessary quality of the services:

- helpdesk and support services;
- network management and administration services;
- directory services.

2.5.1 Helpdesk and Support Functions

Helpdesk and support services are a key requirement in a context of interoperation between multiple independent systems across Europe. System administrators and operation staff supporting their own end-users inside each business partner's domain need a common structure and common procedures for coordination and support of cross-domain data interchange in relation with installation, testing, problem handling and normal operation.

Roles, procedures, responsibilities, contact points, and support staff need to be defined and set up to enable, facilitate and support the interchange of data between European administrations.

2.5.2 Network Management and Administration Services

Network management and administration services are required in a multilateral, international environment, preferably in the way of 'one-stop-shopping', aiming for a high level of operational and administrative simplicity as seen from the user.

2.5.3 Directory Services

In a distributed environment made up of processes collaborating on common business, there is an increasing requirement for distributed directories, allowing services to find current resources and permissions and then communicate with each other via messaging.

2.6 Additional Requirements

2.6.1 Requirements for disabled persons

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. W3C's Web Accessibility Initiative (WAI) and Web Content Accessibility Guidelines (WCAG) address these issues through a combination of technical and educational work. For more information on the Web Accessibility Initiative and the and Web Content Accessibility Guidelines, please refer to section 2.5 of the Annexes to this document.

3 Implementation Principles

3.1 Introduction

Adherence to the architecture described in these Guidelines requires compliance with the principles described in this chapter. Adherence to these principles constitutes the basis of the implementation approach described in the following chapter.

3.2 Definitions

To enable business partners concerned with trans-European networks to enforce their own policies and practices (i.e. technological approach, legal framework, principles of management, etc.) while exchanging or sharing information with business partners, an interoperability model is defined at a Community level that defines a common set of architecture specifications and generic services that expose interfaces and rules at all levels (i.e. technical, managerial and operational). Business partners' networks interface such services at a single entry point of access to the common infrastructure.

The internetworking architecture is illustrated in the following diagram:

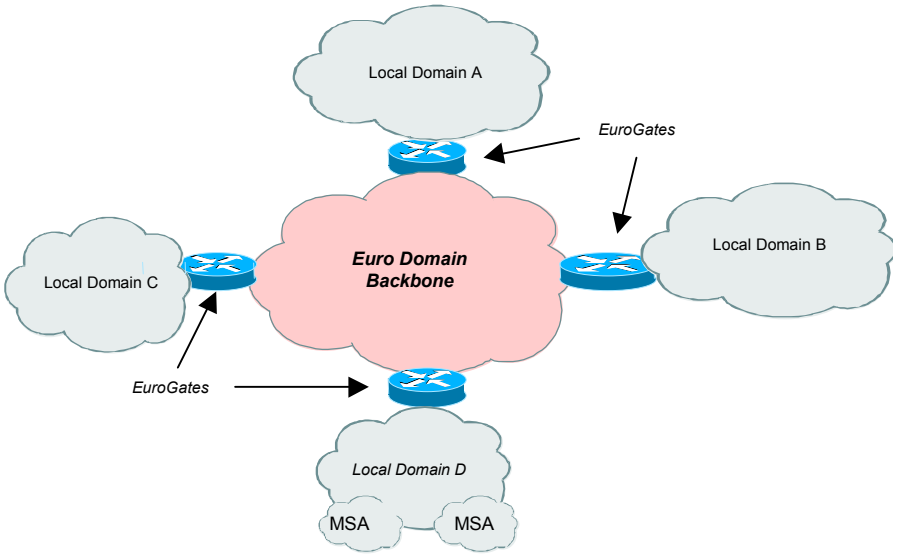


Figure 1, the interoperability model

In the architecture shown above, a homogeneous, Europe-wide central facility is defined as the "EuroDomain", which allows the exchange of data between disparate or similar IT-systems of business partners, called the "LocalDomains".

The EuroDomain is a common set of services that enables transparent links between various LocalDomains of business partners (including whole networks linking multiple partners inside a single domain).

A LocalDomain is a set of homogeneous telematics services. The EuroDomain links individual networks (e.g. LocalDomain "C" in the diagram) but also networks of networks (e.g. LocalDomain "D" in the diagram) used by partner organisations. A LocalDomain can be a national network or an application.

The delineation of responsibility between the EuroDomain and LocalDomains is achieved through an access point, defined as the EuroGate, which is a set of services connecting a LocalDomain to the EuroDomain.

The EuroGate is a key architecture element providing both the flexibility and the managerial and technical independence between the Domains. Each Member State may have its Administrations organised into LocalDomains in any way it wishes. The preferred solution is that a national network is connected to the EuroDomain by means of only one EuroGate. However, if required, more than one EuroGate is possible.

A EuroGate should not be seen as a particular machine, computer or gateway device, but as a set of interface services ensuring exchange between LocalDomains via the EuroDomain services. Moreover, the components of a EuroGate can not be defined in a strict and exhaustive manner as they depend on the services requirements to be fulfilled between a given LocalDomain and the EuroDomain. A common set of services will, however, be constantly available.

In terms of the interchange of data, European Institutions or Agencies are considered as similar independent organisations, having each one or more LocalDomains. Thus, the word "Local" is understood in the extended context of "autonomous organisation", and the LocalDomain is the IT system and network of such an organisation.

3.2.1 EuroDomain

The EuroDomain is a common set of trans-European telematics services, primarily procured on the market from a plurality of service providers. These services are based on specifications and service level agreements as defined by, and agreed upon, the IDA community. Services are designed to enable transparent links between LocalDomains, intended as the information system and networking infrastructure of the European Community organisations. (i.e. Member State Administrations, Community Institutions, EU Agencies.) The EuroDomain consists of:

- a common platform, in terms of requirements, specifications and functionality for trans-European information services,
- a common set of connectivity functions and application oriented services, including various functions for an electronic infrastructure, for the EuroDomain and for LocalDomains,
- a set of interface definitions (protocols, formats, APIs) for the backbone infrastructure of trans-European telematics applications,
- services implementing the above, including exhaustive functional and technical documentation.

The concept of the EuroDomain has been elaborated to provide a single technical reference commonly approved by all connected LocalDomains. This is the way inter-operability can be handled between many heterogeneous Local systems.

For the same reason, the EuroDomain is not directly accessible. Instead, a pair of EuroGates provides the connectivity and inter-operability between any two LocalDomains via the EuroDomain (and to the EuroDomain services themselves). This way, technical independence between the EuroDomain and the LocalDomains is maximised.

Conceptually, the EuroDomain is a single, Trans-European entity providing inter-operability and one stop shopping, with a limited number of service providers.

As part of the IDA responsibility to assist EU organisations with the setting up of trans-European networks, EuroDomain services are defined within the IDA programme and contracted out to service providers through public procedures.

3.2.2 EuroGate

A EuroGate is a set of services, relying on hardware and software features, providing the necessary functions of connectivity and inter-operability between LocalDomains and the EuroDomain. It also serves to define the boundary of responsibility between Domains.

The EuroGate serves the purpose of connecting a LocalDomain to the EuroDomain. If conversions are necessary, these may also be conveniently located in the EuroGate. The EuroGate provides the necessary mapping between users' needs (functionality and quality of service) and available EuroDomain services.

If, for example, a user needs to send a file within a specified time frame and level of reliability/security, then EuroGate calls on the appropriate transmission service in the EuroDomain to meet these requirements. The EuroGate will normally not contain any permanent, specific user data or user processes, except directory and format conversion.

Key roles of the EuroGate, in relation with the EuroDomain, are:

- to support accounting and management functions, as required by all Domains on a common basis,
- to ensure a well defined autonomy and security level of the LocalDomains,
- to serve the EuroDomain as well as the LocalDomains in other aspects according to the responsibilities and the ownership (e.g. system management and administration).

Each EuroGate may include a limited or a full part of the complete EuroGate functionality, depending on the actual requirements of the LocalDomain connected through the EuroGate.

Depending on LocalDomain cases, the EuroGate can be managed, maintained etc., either by the organisation(s) responsible for the LocalDomain(s) which it serves, or by one of the service providers responsible for the access to the EuroDomain. These sets of services are procured from the market on the basis of specifications and service level agreements defined by the IDA administration.

The EuroGate services can be based on a set of IP services that benefit directly from Internet related technology. However, because other communications services and standards are still a necessity in the present situation, these are covered where needed.

Responsibility for, and management of, EuroGates can reside with either the LocalDomain or the EuroDomain, or be shared by both.

3.2.3 LocalDomains

A LocalDomain is a set of telematics services managed by partner organisations (e.g. national Administrations, including networks linking National Administrations inside a single Member State, or EC Services, or European agencies, etc).

A LocalDomain consists of people, resources, information and communication technology equipment and infrastructure, information and data related with a specific set of administrative tasks of a National organisation or a European institution connected to the EuroDomain through a EuroGate. A LocalDomain thus represents the ICT environment for part of one, or several Administrations.

Each Member State may have its Administrations organised into LocalDomains in any way it wishes and may connect these to the EuroDomain through any number of EuroGates, as will best suit its technical and organisational requirements.

Typically, a Member State will thus have a multitude of LocalDomains attached to the EuroDomain through one or more EuroGates. In some cases, one organisation may even choose to appear as more than one LocalDomain if its internal structure allows this.

In other cases, LocalDomains may each be so small that it is more cost-effective to share a EuroGate for their connection to the EuroDomain. This may be the case when a National Network is linking National Administrations, and only one EuroGate is available as gateway to the EuroDomain for these Administrations.

Ownership of a LocalDomain rests with the Administration or institution that uses it.

A LocalDomain may comprise or make use of any type of external services or private networks that fit within the regulations and requirements of its own administration. These external services can also consist of services by means of the Internet, for example as information services or as a means of access to another group of users.

If a LocalDomain decides to use Internet, it is important to realise that direct access to the Internet from the EuroDomain backbone is forbidden.

Therefore, as a general rule, Internet connections will have to be implemented on a LocalDomain, with the definition of a firewalling policy that needs to be notified to all trans-European project partners and stipulated in the co-operation agreement.

3.3 EuroGate services are directly accessible

The EuroGate is a set of services, relying on hardware and software features, providing the necessary functions of connectivity and inter-operability between LocalDomains and the EuroDomain. These services are directly accessible from the LocalDomains.

The EuroGate represents a mandatory and the only path into the EuroDomain. All connections to and from the EuroDomain must go through the EuroGate, which ensures that changes made in one Domain cannot affect the other Domains. Any implementation using the EuroDomain should be able to clearly identify the EuroGate services.

This principle facilitates technical and management independence between Domains, and management of the inter-operability. The boundary between the LocalDomain and the EuroDomain must be clearly identified to allow this technical independence between Domains.

3.4 EuroDomain services are not directly accessible

The EuroDomain services are utilised only through the interfaces between the EuroDomain and the EuroGate. This will facilitate management independence between the LocalDomains and the EuroDomain at the services level, and thus clearly delineate the responsibilities of the EuroDomain. The EuroGate offers services to the LocalDomain at an architecture layer that is equal to, or higher than, that of the EuroDomain, so that the EuroDomain is "hidden" by the EuroGate.

Similarly, the LocalDomain is not directly accessible from the EuroDomain.

3.5 Independence from end-user applications

The EuroDomain and the EuroGates shall remain independent from end-user applications. Therefore, they do not normally contain user data or application specific functions on a permanent basis.

This principle states for the EuroDomain that it is the common environment for all users and applications and that it therefore should not have its operations and management (or cost structure) affected by any one application or its data.

For the EuroGates, this principle ensures that the EuroGate remains dedicated to its function of point of attachment, isolation, and possibly, adaptation. It should not get integrated into the application environment rightly belonging to the LocalDomain, since this would compromise its ability to isolate between the LocalDomain and the EuroDomain.

3.6 EuroDomain appears as a single entity

EuroDomain service providers are contractually required to collaborate to make the EuroDomain appear to users as a single entity. They should share transparently operational data, user data, and traffic data, and should arrange a one-stop-shopping system.

The objective of this principle is to achieve full any-to-any communication while maintaining service provider competition and user choice.

3.7 LocalDomains enter into proper collaboration agreements

LocalDomains are invited to establish collaboration agreements in those projects in which they exchange data across the EuroDomain. In addition to those elements of particular significance for the applications in question, it should establish minimum requirements of operational significance, such as opening hours, software version control, troubleshooting arrangements, etc. Common elements (to be developed) should likewise be included with respect to the collaboration with the EuroDomain services and the management of the EuroGate.

3.8 Adequate security policies must be defined

Each sector must consider the need to set up a security policy that must encompass all layers of the architecture. For more information on security, please refer to section II of this document.

3.9 Charging policies must be defined

Trans-European network design, set up and operation are the joint responsibility of all partners concerned. Charging policies must be defined at the project planning stage and included in contacts and agreements. In support of the applicable charging policy, EuroGate-level accounting mechanisms must be defined in order to make information available to partner organisations.

3.10 Maximum use of generic services and common tools shall be promoted

Use of generic services and common tools is a requirement of the Interoperability Decision. Trans-European projects should use such services as much as possible and provide a clear rationale for a different approach.

Generic services are defined in article 2 of Council Decision No 1720/1999/EC as telematics network functionalities that meet common user requirements, such as data collection, data dissemination, data exchange and security.

Generic services provide solutions for sectoral needs. Use of generic services should lead to the promotion of interoperability within and across sectors, the emergence of a common telematics interface and substantial benefits for Member States and the Community, spread of best practice and eventually, the extension of networks to industry and the European citizen.

Generic services are provided, managed, run and funded by the Commission. Currently available generic services include the implementation of the network services of the architecture, and these Architecture Guidelines.

For more information on available Generic Services, please refer to the Catalogue of Generic Services.

Common tools and techniques should be compliant with the Architecture Guidelines as well as with the generic services. The development and use of common tools by sectoral networks, as well as the spread of suitable solutions, is encouraged.

For more information on available Common Tools and Techniques, please refer to the Catalogue of Common Tools.

Section II

Implementation Approach and Guidance

4 Implementation Approach

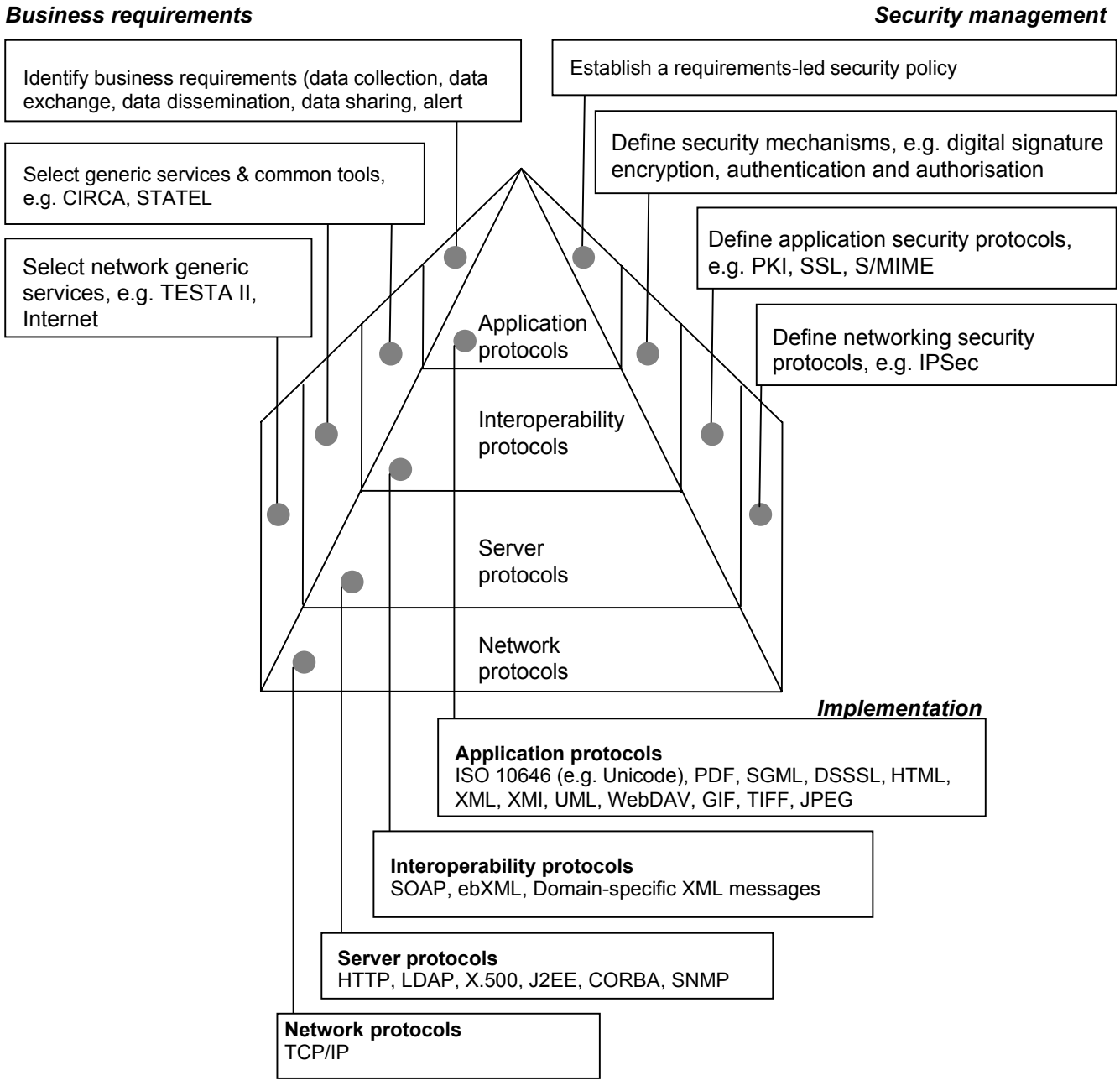
4.1 General architecture and recommended technologies

The following diagram illustrates the IDA architecture interoperability model and its recommended technologies. The architectural components are described in detail in the following sections.

The model defines a layered structure of which each element uses services provided at the lower level by means of standard interfaces.

The diagram provides three dimensions of a project, each one represented on a face of a pyramid:

- ***business requirements***, involving the definition of a suitable implementation approach;
- ***security management***, involving a security policy that meets the security requirements and a set of security mechanisms that enforce the policy on the trans-European network;
- ***implementation***, involving the integration of building blocks that meet the various requirements.



4.2 Application and Content Interoperability Services

Two main application models are commonly enforced in trans-European projects:

- **Transactional model**, in which centralised servers running on a LocalDomain are designed to grant access to users at counterpart LocalDomains by means of a web interface. Business partners input, query and retrieve information from the web. The central service is built around a standard SQL-based relational database system if itemised data is concerned and/or a document management system for document-based information. Ideally, whatever the information type, XML is used to handle information structures according to a model that is shared among all the business partners.
- **Application-to-application-type communication model**, in which business partners independently handle their own data and use a facility when needed to extract data from the database and to send information to the intended recipients. A counterpart receiving function enables data to be included in the local database. A common format is decided for data transmission that leaves parties fully independent as to managing data internally. Again, XML provides the foundation for data handling.

The above two models are not used rigidly. Often trans-European networks enforce varied combinations of the two models. A single trans-European application might involve gathering the information from all partners using application-to-application communication, storing the information in a centralised database and offering query functionality to designated partners from the web. Typically, publicly available information can be made available to a wider user community on the Internet. Also, in the case of application-to-application communication, requirements for third-party notary services are likely to make the designer opt for a centralised service that keeps track of the message flow on a LocalDomain.

Web, Java and XML technologies make up a coherent architecture supporting the two above models on the IDA architecture.

4.2.1 The Transactional Model

To build up transactional applications giving access to a centralised database, a web-based model is adopted.

To ensure ubiquitous availability across independent EU organisations while easing development and deployment, a simple web model based on a standard client (browser) and a standard protocol (HTTP) is recommended for trans-European networks. Applications are built on top of this model using middleware based on scripts.

The display part is based on HTML 4.0 and higher. A script engine associated with the HTTP server carries out script execution. Local validation is performed on the client system using a script language such as Javascript.

This architecture is the only suitable set-up for supporting a large-scale deployment without client installation and should be used whenever possible.

The two main benefits of this architecture are the universality of the client and its simplicity. Only information systems that conform to this architecture will be accessible to a large public or to mobile users and will interconnect with external systems without a major redesign.

Data structures are handled via XML, based on DTDs or XML schemas agreed upon by the user community. Rendering is entrusted to XSL. Parsing is done at server side using Java.

Interface complexity is conveniently handled using technologies such as the following.

- **DOM -** Document Object Model - a language based on a W3C standard that makes it possible to programmatically access and update via scripting languages (e.g. JavaScript) the content, structure and style of a document (HTML, XML). Attention will have to be paid to ensuring that the set of DOM functionality used is widely supported in commercial browsers.

- **Cascading Style Sheets**, a W3C standard which defines a style sheet language that allows authors and users to attach style (e.g., fonts, spacing, aural cues and other properties) to structured documents (e.g. HTML documents and XML applications).
- **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).

Open source technology offers extra means to handle web interface complexity. Mozzilla has defined **XPToolkit** as a specification that leverages XML, DOM, XUL and CSS and combines them to support the implementation of top-quality user interfaces. XPToolkit is a collection of loosely related facilities, from which application writers can pick and choose, providing a platform-independent API to some commonly exploited functionality.

In developing simple, web model-based applications, special consideration should be given to the integration of the browser with printers, as this area is not covered by web standards awaiting the emergence of the Printing Internet Protocol. In the meantime, the PDF format or equivalent non-revisable format is recommended for printing documents, while printing HTML pages will require some testing with various printers.

Whenever the required complexity of the interface requires supplements to the browser's native interface, Java applets may be used on the client side with the following recommendations:

- anything that executes within the browser's sandbox is permitted;
- Java applets that are recognised via a digital certificate or a safe channel deployment are permitted;
- the use of Java based supplements should be minimised whenever the target population is unknown because the dependence of the Java virtual machine on the browser brand and release number.

The web servers hosting the HTTP processes and the application servers supporting the business logic and access to the SQL database must be independent of any operating system.

There is, however, one limitation to this architecture model: the non-session nature of the HTTP protocol does not always allow the implementation of transactions and of network recoveries for complex iterations. This means that complex transactional systems may not be implemented on a strict web architecture.

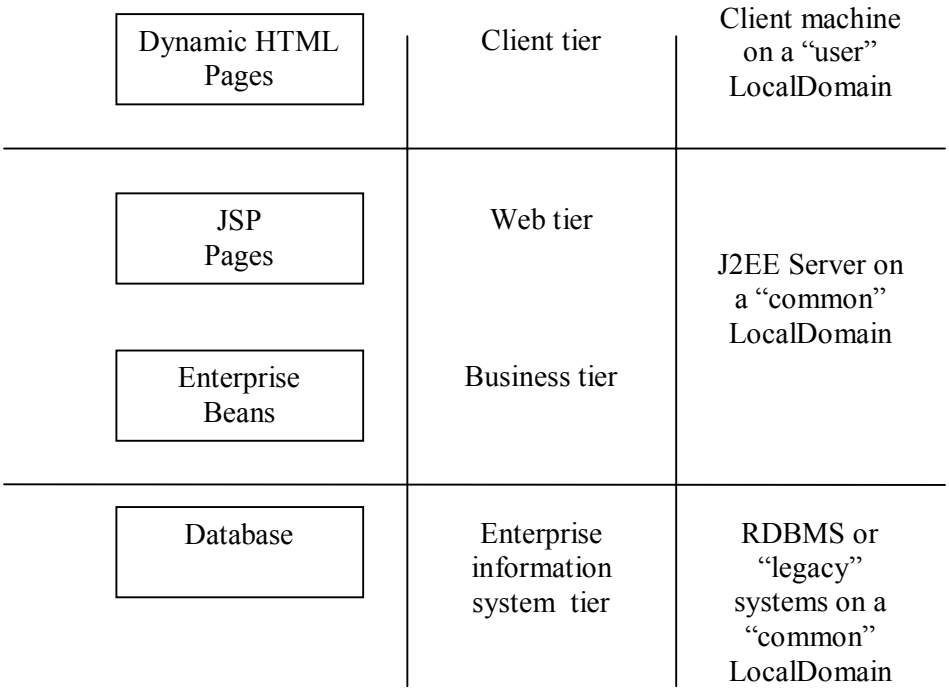
When the business complexity at hand cannot be dealt with using the simple HTTP model, the following Java-based technologies offer a suitable, feature-rich reference application development platform:

- Applets, providing client components;
- Java Servlet and JavaServer Pages (JSP) providing web components;
- Enterprise JavaBeans (EJB, enterprise beans) providing business components;
- Enterprise Information System (EIS) software, providing access to information.

The server-part components are grouped into the J2EE set of specifications (Java 2 Enterprise Edition). On account of its wide-industry support and the level of maturity reached, J2EE is recommended as the reference specification for component-based application design, development and deployment over the IDA architecture. Other reasons for recommending this architecture include:

- the effectiveness of the EJB components, that are designed to have developers just deal with the business logic at hand, because the "container", i.e. the environment in which a single EJB is run, transparently handles complex management tasks (i.e. access control, transaction management, database access) without any API to be explicitly called. EJBs provide a portable, vendor-independent environment for distributed objects;
- native support of XML as a standard means for interoperation between independent systems;
- the capability to isolate, in a three-tiered model, the client aspects from the business logic and data access logic that are implemented by session beans and entity beans.

The J2EE components map out onto a typical IDA Trans-European network as follows:



For additional, detailed information on J2EE specifications, please refer to Annex A, paragraph 2.6.4.

4.2.2 The Application-to-Application Communication Model

The J2EE distributed model is suitable for implementing services on a "common" LocalDomain enabling transactional access from all the LocalDomains where the intended users belong – such as in the case of a centralised database (run e.g. by an EU Agency) that is fed and/or searched by users from disparate LocalDomains. The distributed nature of the J2EE architecture may be taken advantage of to integrate resources that are located on multiple systems, as long as such resources pertain to a unique administrative domain.

These guidelines discourage the use of the model to implement distributed applications across collaborating LocalDomains. Tight forms of application binding components through firewalls must be avoided because of requirements for decentralised responsibility and autonomy as well as for security (especially privacy and integrity.) An organisation must keep full control (and responsibility) over the use of a LocalDomain backend applications.

As a consequence, when a business process requires partner organisations to collaborate directly, without any intermediate organisation's support, and/or when the information that is to be exchanged is independently processed inside the partners' infrastructure, these guidelines recommend that a business-to-business (B2B) model is enforced. This model is based on loosely coupled independent functions running on collaborating LocalDomains. Due to this limitation, this type of business requirement has consistently been dealt with using an EDI-type of approach that involves either using EDIFACT technology based on commercial platforms or developing proprietary business messages (SGML-based) plus conversion-translation processes at the concerned end points. The enabling communication technology used was asynchronous and e-mail-based.

While the above technologies are still covered in these guidelines for backward compatibility, the reference architecture for the next-generation trans-European networks is based on current, industry-driven business-to-business models that consistently use XML as the exchange language on top of HTTP and SMTP. The latter are the protocols best suited to support information exchanges across corporate firewalls.

XML defines document structures through marking up textual information according to its semantic content. XML enables inter-organisation system exchanges to be implemented on top of a message oriented middleware infrastructure built on the basis of SMTP or HTTP + XML. This is the only standard infrastructure that is sufficiently flexible to cover all types of devices and accommodate for various latency times.

However, interconnection of systems between partner administrations or other institutions requires not only an agreement on a shared data description mechanism and on a set of protocols, but also on the business process. XML, SOAP and ebXML provide the ideal foundation for business-to-business (B2B) exchange of information over the trans-European architecture.

While the use of XML alone on top of customised mechanisms to exchange data can be considered on a case-by-case basis, especially as long as the target foundation is not yet fully mature, for large-scale development of interoperable B2B these guidelines stress the need for:

- formalised business protocols focusing on their externally visible behaviour;
- standard schemas for business documents including metadata on context information (e.g. partners' profile, document types, process types, sequence of messages forming a unique process instance, timing constraints, error management, etc.)
- specification of the underlying communication infrastructure requirements including quality of service;
- specification of security requirements such as signatures, encryption and authentication, and the reference technology (e.g. XMLDSIG or S/MIME.).

SOAP

SOAP (Simple Object Access Protocol) is a forthcoming W3C standard defining a distributed application model that uses XML for enabling applications to communicate with each other over a network. SOAP provides a simple and lightweight mechanism for exchanging structured and typed information between applications in a decentralised, distributed environment. SOAP does not itself define any application semantics such as a programming model or implementation specific semantics. Instead of this, it defines a simple mechanism for expressing application semantics by providing a modular packaging model and encoding mechanisms for encoding data within modules. This allows SOAP to be used in a large variety of systems ranging from messaging systems to Remote Procedure Calls (RPC). SOAP leverages HTTP and XML, providing a guarantee for interoperability.

Basically, SOAP extends HTTP, which was only designed as a mechanism for passing files from servers to clients, not for application-to-application communication. SOAP adds a set of HTTP headers and a rich XML payload to enable complex application-to-application communication over the Internet. Messages are formatted with XML.

The stated goal of the SOAP specification is two-fold:

- To provide a standard object invocation protocol built on Internet standards, using HTTP for transport and XML for data encoding. The client sends a request to a server to invoke an object, and the server sends back the results.
- To create an extensible protocol and payload format that can evolve over time.

SOAP consists of three parts:

- the SOAP envelope construct defines an overall framework for expressing the contents of a message, who should deal with it, and whether it is optional or mandatory;
- the SOAP encoding rules define a serialisation mechanism that can be used to exchange instances of application-defined data types;
- the SOAP RPC representation defines a convention that can be used to represent remote procedure calls and responses.

The relevant SOAP specification is SOAP 1.1 with attachment messaging.

ebXML

ebXML is a global electronic business standard that is sponsored by UN/CEFACT (United Nations Center For Trade Facilitation And Electronic Business) and OASIS (Organisation for the Advancement of Structural Information Standards). ebXML defines a framework for businesses to conduct transactions based on well-defined XML messages within the context of standard business processes which are governed by standard agreements.

The ebXML technical infrastructure is composed of the following major elements:

- Messaging Service - This provides a standard way to exchange XML business messages between organisations. It provides a protocol-neutral framework for exchanging a payload reliably and securely, supporting SOAP as the underlying platform for message exchange. It also provides means to route a payload to the appropriate internal application once an organisation has received it.
- Registry services, to handle information on XML schemas of business documents;
- Partner profiling services, based on so called Collaboration Protocol Profile (CPP). These services allow partner organisation profiles to be described (by means of DTDs and W3C XML schemas) in terms of which business processes an organisation supports, its roles in that process, the messages exchanged, file transport protocols used, network addresses, security implementations, transport mechanism for the messages, etc.
- Process definition, using a Business Process Specification Schema (BPSS), that defines how a business process is to be conducted, e.g. the roles, transactions, identification of the business documents used (the DTDs or schemas), document flow, legal aspects, security aspects, business level acknowledgements, and status. A Specification Schema can be used by a software application to configure the business details of conducting business electronically with another organisation.

ebXML is designed to serve e-business requirements on a global scale. Therefore, on top of the above infrastructure, ebXML defines processes to enable business partners to meet in the first place, to negotiate terms of collaboration and even to commit their own organisations electronically. Such extra functionality is outside the scope of these guidelines that serve requirements of a specific trans-European network community.

Integration of XML-based exchange mechanisms on a LocalDomain

The combination of J2EE and XML provides a sound and sufficiently mature foundation to build trans-European networks.

Currently, two J2EE-based systems can exchange information using custom-designed enterprise beans that retrieve XML messages from a B2B counterpart's URL (even via simple JSP pages), parse the XML message using DOM via the JAXP API, and encapsulate XML data in the J2EE environment.

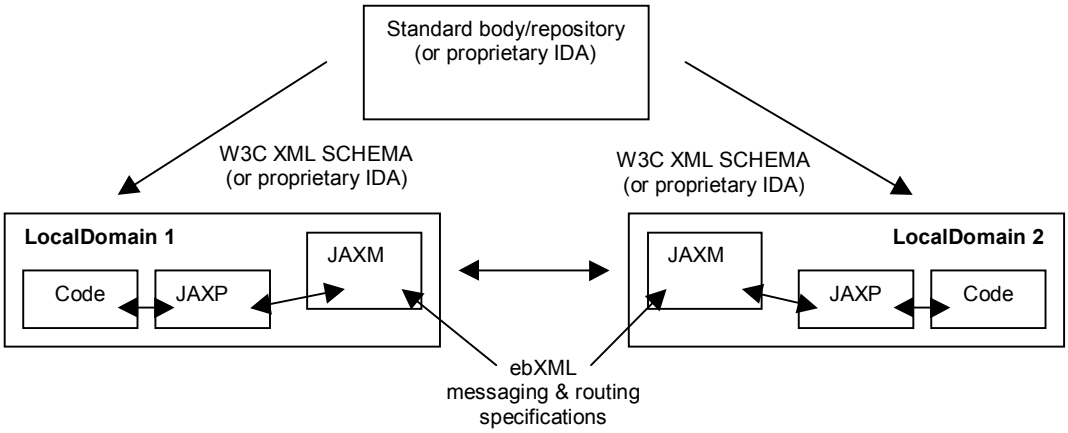
Extensive data transformation and manipulations may be done at each end using XSLT, a transformational language standardised in W3C, that can be used to transform XML data to HTML, PDF, or another XML format. For example, XSLT can be used to convert an XML document in a format used by one LocalDomain to the format used by another LocalDomain.

This technology may be used to integrate an XML format conversion tool onto a EuroGate, allowing LocalDomains to use their own technology while fully interoperating with one another.

While providing the basis for open trans-European interoperability, this setup requires implementers to develop a great deal of code to handle the business flow, XML parsing and data extraction. However, key components of the Java/XML architecture are expected to be released shortly. These components will streamline the entire B2B process and make it straightforward to deploy. The following two specifications are currently undergoing the Java community process.

- JAXB (available as an Early Access release inside the Java community process) - enables two-way mapping between XML documents and Java objects, offering a schema compiler and a schema binding language. The compiler automatically generates Java classes from XML schemas with no need for parsing code. (The compiler automatically checks for error and validity, making sure that only valid, error-free messages are processed.)

- JAXM - enables the packaging, routing, and transport of XML business data using either HTTP, or SMTP, or FTP as underlying protocols. JAXM is designed to fully support ebXML transportation, routing and packaging (TR&P) specification, which provides a SOAP-based widely industry-supported standard for simple, robust, low-cost, and reliable XML-based messaging platforms. JAXM implements SOAP 1.1 with attachment messaging.



The combination of ebXML, XML and J2EE standards set out the following reference architecture for IDA trans-European content/application interoperability:

4.2.3 The Web Services Model

An innovative model is surfacing in the e-business world that uses existing standards such as SOAP for interoperability on HTTP, providing interoperation of web services. This model makes it possible to set up a business process that relies on steps executed by web services in a coordinated manner. In the business world, this approach is important to enable contributions by independent organisations to the business process (a typical example is a purchase from the web: as the shopping list is ready, the credit card of the customer needs to be checked by a different actor – a bank – whose service can then be invoked online by the shopping application. On conclusion, the process control is returned to the merchant organisation application for follow-up).

This model uses the following industry standards:

- Web Service Description (WSDL) - A Web Service has to be described to enable organisations to use it. WSDL is used to describe a Web Service. The description of a Web Service indicates this Web Service's functions, such as the input/output parameters and transport protocols.
- Web Service Publication and Discovery - An organisation needs to publish the Web Services that they own, for other organisations to discover them. Universal Description, Discovery and Integration (UDDI) specification is used to publish a Web Service to a central UDDI Repository. Other organisations can then perform UDDI operations to access the UDDI Repository, and discover Web Services that are of interest to them.
- Web Service Invocation - Once an organisation has discovered a Web Service via the UDDI interface, and has made a decision to use it in their application, they need to invoke the Web Service. The Web Service invocation is done via SOAP over HTTP.

4.2.4 Electronic Document Management Systems and Workflow Systems

Electronic Document Management Systems (EDMS) and Workflow systems constitute an infrastructure supporting the lifecycle of documents. EDMS is the document repository and the workflow organises the document flows.

There are various categories of document repositories depending on their sophistication. EDMS repositories offer more or less complex document input mechanism, versioning systems, integrity controls, search tools, a management system, format viewers and file integrators into folders.

There are various categories of workflow systems depending on their sophistication. Workflow systems offer more or less complex document routing and flow control mechanisms, built in tasks and role descriptions, a programming language and interfaces to other systems.

A distinction can be made between:

- Procedural EDMS or workflow systems which are linked to administrative procedures and monitored by an information system. They are either implemented in-house or by customising a package using high level programming.
- Ad-hoc EDMS or workflow systems, which are, linked to collective office automation systems.

There are many different approaches competing for market shares as far as procedural EDMS or workflow systems are concerned. This situation results from the too loose definition of EDMS or Workflow, from the sheer heterogeneity of user needs (time constraints, level of sophistication) and also from the historical background of the solutions: specialised EDMS or Workflow vendors, DBMS extensions, new web-content management packages, electronic commerce newcomers. Despite the efforts of the Workflow Management Coalition (WfMC) and of the W3C, a very limited number of implementations of standards is available that provide adequate interoperability between workflow systems.

The IDA project MoReq (**Mo**del **Req**uirements for the Management of Electronic Documents) specifies detailed functional requirements for the management of electronic records. It contains a model of how file plans, files, records, etc. relate to each other. It is applicable both to electronic and hybrid files (i.e. files that contain both electronic and paper records). MoReq assumes that this model and these requirements will be implemented by a system called an ERMS - Electronic Records Management System. However, it does NOT specify the ERMS - only what it should do. How the ERMS is implemented is the responsibility of the user. MoReq also includes a comprehensive metadata model for managing records.

The MoReq model can be downloaded from the IDA web site (http://www.europa.eu.int/ispo/ida).

However, a WfMC standards-compliant solution is recommended and a web-based interface should be seen as a key requirement for trans-European networks.

For the collaboration with external partners or the support of meetings requiring archiving or versioning, pure Web based solutions will have to be used, even if they are less rich in functionality or less well integrated with the desktop. Common workspaces are created for sharing, and possibly using common tools.

4.3 Network Services

EuroDomain internetworking services between LocalDomains are built on top of the IP generic standards.

The choice of internetworking services and service levels to be enforced in a new trans-European network project depends on specific requirements in areas such as security (e.g. requisite confidentiality level), application model (i.e. transactional or business-to-business asynchronous exchange), performance, etc.

The following diagram illustrates two alternative routes available to sample Administration "A" and "B" that need to interoperate. The top part of the diagram configures a private, high-speed and secure interconnection, while the bottom part relates to a cheap but readily available, public route, i.e. the Internet.

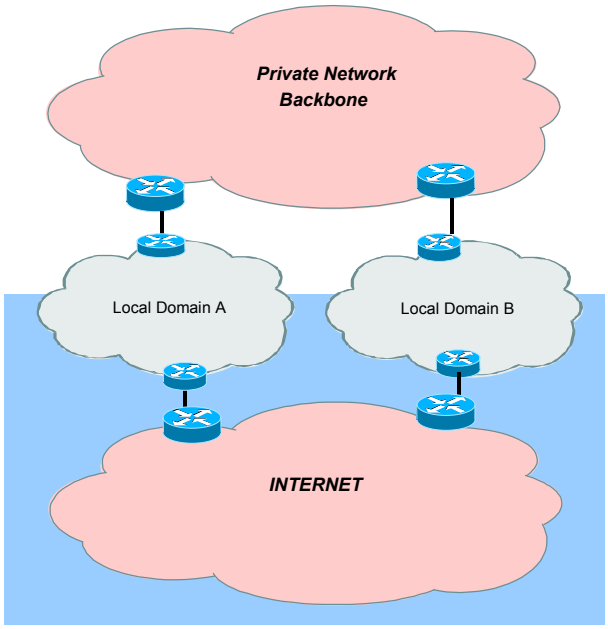


Figure 2, Public and private networking solutions

The public network, implemented by means of the Internet, allows immediate and inexpensive internetworking because all organisations involved in a trans-European network already have controlled access to the Internet, each using its own established service provider.

The private network is a Closed User Group and can only be accessed by user organisations who, after having been admitted as a user. After having been granted access, users can benefit from the higher performance and security of the network. The organisation that manages the private network usually offers additional services such as management, maintenance and assistance.

For the time being, the scope of these guidelines mainly focuses on the private network, even though the users of the private network can use the Internet to exchange information with some users, while at the same time using the private network to exchange this same information with other users.

The rationale behind the focus of these Guidelines on the private network is the fact that the Internet is a public network, and its access and use is considered as part of the internal policy of a local administration.

However, with complete standardisation of VPN protocols, the distinction between the two alternative routes will probably loose significance. In future, local Internet service providers may be able to jointly provide the same end-to-end quality of service that is currently provided at the level of the private network, bridging security and performance gaps. By that time, the guidelines will cover interoperability through VPN standards, focusing on SLAs with multiple Internet services providers.

The Private Network underlying the internetworking architecture covered by these guidelines is described in the following sections. Network services are offered at EuroDomain level as generic services (referred to as TESTA II) by a selected service provider under a framework contract with the EC.

TESTA II provides IP backbone and backbone access services dedicated to inter-administrative traffic, with guaranteed levels of performance. EuroDomain IP backbone services are designed for connecting single users, single organisations, and networks of organisations (e.g. a National public sector network) in a closed user group (CUG), enabling any-to-any connectivity within the CUG.

Different classes of services are supported which are delivered and managed according to Service Level Agreements (SLA) that the LocalDomain manager signs with the EuroDomain service provider.

Implementers are invited to select such services from a catalogue that is available to trans-European projects.

4.3.1 Testa II

TESTA II consists of a set of services that are available to all Trans-European projects under a framework contract between the EC services and a service provider placed via public procurement procedures. The TESTA II catalogue includes all services (i.e. both backbone and backbone access) that are required to set up the EuroDomain internetworking infrastructure and the EuroGate services for a trans-European project, providing guaranteed service levels that are incorporated in a Service Level Agreement.

The network relies on the standards-based Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite, available from the EuroGate. The network is not connected to the Internet. Primary service characteristics are:

- trans-European coverage including EU, EFTA, EEA and CEECs;
- designed for connecting single users, single administrations, and networks of administrations in a closed user group (CUG);
- based on routers as interface;
- any-to-any connectivity within the CUG;
- support of different classes of services which are delivered and managed according to Service Level Agreements (SLA);
- backbone access allowed via dial-up or leased lines; support of ISDN, PSTN, ATM and Frame Relay technologies; open to evolution (SDH, xDSL);
- built-in security features (access control, physical separation from the Internet, use of Tag Switching for Virtual Private Networks -TAG-VPN- and announced migration to Multi-Protocol Label Switching - MPLS); additional firewall and cryptography services are available on-demand;
- value-added services including Electronic mail (e-mail), Domain Name Server (DNS), web repository and web hosting services; telephony and videoconferencing services - as future perspective;

The TESTA II service offering is complemented by consultancy services, available on-demand, to help the migration towards TESTA and to monitor the service quality.

4.3.2 Network Addressing

LocalDomains are interconnected through the EuroDomain using TESTA II registered IP addresses. The entry point to TESTA II is configured by means of Network Address Translation (NAT), i.e. a LocalDomain's internal IP addresses are translated into TESTA II registered IP addresses.

Addresses are assigned in an overall addressing scheme that covers the European countries and European institutions. The address allocation rules ensure that address space is allocated equally and flexibly to each country or institution.

Network Address Translation (NAT) is used throughout the TESTA II network to translate source and destination addresses between private ranges in the LocalDomains and the registered addresses. The Network Address Translation takes place at the EuroGate router in the LocalDomain, i.e. IP addresses are assigned virtually at the router but are not used internally.

Address ranges are assigned according to the requirements of the LocalDomain connecting to TESTA II. Only the registered address range is routed over the TESTA II network (EuroDomain), which means that Internet traffic from LocalDomains is not routed over the EuroDomain.

4.4 Security Services

4.4.1 General Issues

Security is a combination of management practices, awareness, policy and training with technology that makes security measures effective. Trans-European networks should be built and run within a clear security policy, that is referred to as a set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed.

An integral part of the security policy is the infrastructure security policy, defining security-enforcing mechanisms that are enforced by specialised software/hardware components. In a trans-European network context, security spans several layers, as shown in Figure 3.

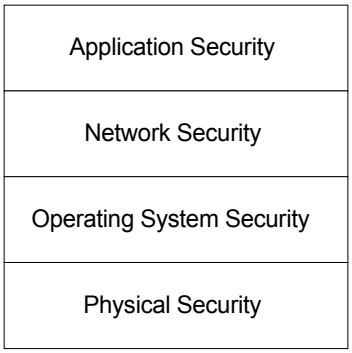


Figure 3, Security layers

Physical security plays an important role in the security process, as this is the first layer that protects systems. It prevents intruders from entering premises, which would enable them to guess important information about systems, such as passwords and sensitive information. Furthermore, it reduces the risk of intentional destruction of hardware or software components.

Operating Systems (OS) or host-based security is the next layer of security. Passwords and a password policy should be implemented and unused accounts should be deleted. System administrators should keep security mechanisms updated by applying the latest security patches and controls using the most recent release of the OS.

Network security is also to be taken into consideration. Intranet/Internet/Extranet security with firewalls, TCP/IP-based security and other features provide a requisite assurance level. Encrypted connections and/or channels provide transmission confidentiality.

Application security is the top-layer, for securing user accesses to applications, authenticating them and providing means of identifying proof-of-origin for messages, transactions, etc. Application security sometimes relies heavily only on OS security. A more in-depth look at OS security functionalities could help to devise an application security policy, which would re-enforce global security.

To implement efficient security, all levels must be considered. A security strategy should recommend securing all layers to the maximum possible extent, rather than relying on a single component.

In this context, the recommendations of standard BS7799 - Information Security Management (1999), currently being 'fast-tracked' to become an ISO standard, are relevant. BS 7799 provides 100 security guidelines structured under 10 major headings to enable organisations to identify the security controls that are appropriate to their business or area of responsibility. As well as detailing security controls, BS 7799 also provides guidance on related security issues, such as policies, security awareness, business continuity planning, etc.

The SecLeg project provides a framework for drawing a security policy for a trans-European project.

4.4.2 Information System security implementation

A global end-to-end Information System (IS) security implementation between two LocalDomains using the EuroDomain relies directly on three implementation components (see Figure 4):

- the EuroDomain security implementation to be built by the EuroDomain Service provider;
- the LocalDomain security implementation, comprising application security and network security implementation to be eventually built by the application-owner, considering the former as a minimum-level implementation;
- the Security Service Level Agreements (SSLA) to be established with the partners in the business information exchange relevant to the IDA application.

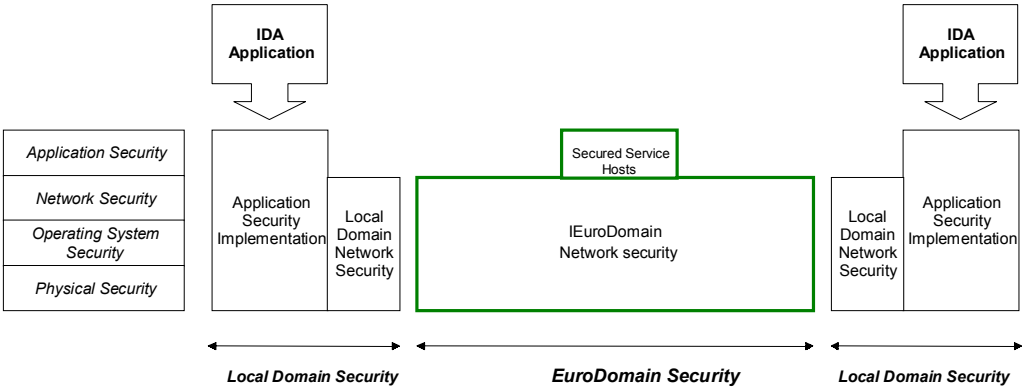


Figure 4, IS security implementation

It is important to state that security implementations must coexist, interwork and be policed within specific Security Service Level Agreements between the LocalDomain and the EuroDomain Service provider.

In those Security Service Level Agreements, it is also important to cover 'the indirect component of security' by referring to specific security policies that the LocalDomain and the EuroDomain Service Provider apply to external third parties.

4.4.3 Application security scope

Any application security policy for an application located inside a LocalDomain and using EuroDomain should appraise and include the security level given by EuroDomain and define, by deduction, its own security ruling.

For example, an application might consider using IPSEC functions to ensure that the IP addresses of the application hosts are not known, even with 'sniffing or eavesdropping' techniques (technical terms for listening to the network and capturing data) from within the EuroDomain.

The following table shows the security layers to be considered for an effective application security at the level of the LocalDomain.

Security Layer	Protection needed	Where
Application Security	Yes	For *application user access* and for access to IP generic services carried over EuroDomain.
Network Security	Yes	For monitoring and *auditing network accesses* from/to the corporate networks, regarding EuroDomain and other external networks.
Operating Systems Security	Yes	For *application servers* in LocalDomains.
Physical Security	Yes	For *accessing application* environment.

In each security layer, assets need to be protected, regarding the potential threats.

4.4.4 A PKI for trans-European projects

The IDA PKI for Closed User Groups project (PKICUG), launched in January 1999, provides a PKI to secure the information exchanged between the trans-European network partner organisations. The IDA PKI provides all the necessary services for the management of electronic certificates (creation, revocation, and renewal). It is complementary with the infrastructures set up by individual partner organisations (e.g. the European Commission).

By setting up a Public Key Infrastructure IDA has provided an interim solution to trans-European network security requirements. When the PKIs used by participants in IDA networks are fully interoperable, the future of the IDA PKI will be subject to review.

The IDA PKI provides X.509v3 electronic certificates that can be used: (a) to protect client/web server exchanges, including authentication, that use the SSL protocol, and (b) for encryption and authentication of e-mail exchanges that comply with the S/MIME protocol.

4.5 Accounting Services

EuroDomain and EuroGates support accounting and billing functions through the generation of usage information based on various sorts of resource utilisation information. Parties in a trans-European network agree upon mechanisms to be implemented to handle the following elements.

Accounting - accounting determines the process of collecting information in relation to a service's utilisation, expressed in resource usage or consumption. Accounting means monitoring the resource use according to agreed criteria and processing the information into values that are suitable for use of a charging system. The values are stored within an accounting record that forms the basis for charging and billing. Guidance should specify which system should manage this information and in which manner.

Charging - Charging is the process of calculating the cost of a service applying a unit price on a given set of accounting records relating to a user. Charging is a function which translates accounting technical values into monetary units.

Pricing - Pricing is the process of setting a price on a service. Prices are set on predefined services, where the quantity used is measured, e.g., in units, time, distance, bandwidth, volume, or any combination thereof. These basic quantities to be priced are obtained from accounting devices.

Billing - Billing denotes the process of transforming the collected charging information for a customer to his bill. It includes the process of listing for a customer all charging information being contained in charging records which were collected over a time period, i.e., one month. The bill summarises all charges and indicates the amount to be paid. It may identify the method of payment chosen or selected, and it is transferred electronically or on paper to customers.

Sectoral projects must include mechanisms for collecting and logging this information. On a common LocalDomain, specialised functionality will be implemented to enable collection, processing and distribution of data. Processing of utilisation information should be clearly separated from the billing/charging policy. Formats and mechanisms for distribution of this information are decided at project onset and must be incorporated in project management procedures and plans.

4.6 Logging Services

The EuroDomain and the EuroGates should support common tools and mechanisms for logging EuroDomain service utilisation information, to be logged in defined formats. The complete utilisation information logged needs to be collected and processed at regular intervals through the use of common network management tools.

Utilisation information will be collected centrally and logged according to time stamps, used services, initiating and responding addresses, duration etc. This information represents the basic EuroDomain utilisation information.

4.7 Helpdesk and Support Services

The basic principle of EuroDomain helpdesk and support services should be that:

- end-users in the LocalDomain are supported by the system Administration staff of the LocalDomain itself. The end-user helpdesk is within the LocalDomain;
- system administrators of LocalDomains are supported directly by the EuroDomain support functions and helpdesk.

Application of these principles implies that the EuroDomain support and helpdesk never interacts directly with end-users of the LocalDomains, only with the system Administration staff of LocalDomains.

The support staff of the EuroDomain should be able to guide the administrator of the LocalDomain and should be educated and equipped to perform the first level diagnosis of any problem in the use of EuroDomain services and its components. The support function should also be able to connect the local system administrator to the helpdesk of another LocalDomain in case this is required, e.g. in relation with access to common databases and applications.

A responsibility scheme for support, escalation procedures and helpdesks in the EuroDomain and LocalDomains needs to be defined in detail in relation to the definition of contracts with EuroDomain service providers. The responsibilities for services could be organised as follows:

Local end-user	**LocalDomain support/helpdesk**	**EuroDomain support/helpdesk**
General: User support from local Adm. Staff	**General:** Support the local end-users, interact with EuroDomain staff	**General:** Support the LocalDomain system/network Adm. staff
Installation: Training in end-user tools	**Installation:** Purchase, contracts, installation. Tests, sign off with HW/SW vendor and with EuroDomain.	**Installation:** Deliver EuroGate specifications Connect EuroGate Guide and participate in tests
Normal Opr.: Normal use of end-user tools	**Normal Operation:** Support end-users, back-up, definition of access rights monitor EuroGate and local system.	**Normal Operation:** Routine procedures, monitoring, accounting info, general support.
Configuration: Request local staff to perform changes	**Configuration:** Perform on-going changes, and report changes to the EuroDomain. Also, carry out changes following from reconfiguration in the EuroDomain	**Configuration:** Register changes in LocalDomains and ensure that the changes are consistent (i.e. that the changes do not violate the consistency) and that they comply to the general IDA requirements (e.g. on addresses)
Problem Hdl.: Reporting to local staff	**Problem Handling:** Troubleshooting, decide whether to involve EuroDomain or local HW/SW vendor or both.	**Problem Handling:** Support the LocalDomain system adm. staff in troubleshooting. EuroDomain vendor contacts.
Other mts.: As guided by LocalDomain	**Other matters:** First level end-user support	**Other matters:** First-level support to local adm. staff, possibly second level support to end-users

4.8 Management Services

Trans-European networks should facilitate management of the LocalDomain-based customer environments. Processes and mechanisms must be defined to ensure collaboration and interaction between EuroDomain and LocalDomain service providers, to enable:

- Network planning and network address planning, installation, configuration and documentation for additional users.
- Testing and problem handling.
- Network management and operations control.
- Performance management and quality of service monitoring.
- Security services.
- Network information services of various kinds.
- End user training and support, assistance to LocalDomains.
- Taking part in new developments and integration and testing of new technology.
- Internal and external coordination of/participation in other EuroDomain related activities.

To this end, LocalDomain and EuroDomain Managers need to agree on network management standard applications (i.e. SNMP-based) as well as on procedures (i.e. definition of standard performance / statistics information, schedule, technical help-desk service, etc.) to set up a coherent management framework towards customer organisations.

In particular, at EuroDomain level, procedures and organisational relations need to be established to secure that the management centre appears as one logical entity, based on the close collaboration between the system and network administration centres of the service providers in the EuroDomain.

WBEM standards should be considered for managing system and network resources that are part of a trans-European network. WBEM (Web-Based Enterprise Management) is a major industry standardisation effort, run by the Distributed Management Task Force DMTF, www.dmtf.org, an industry alliance of more than 200 companies). The wide recognition of WBEM is confirmed by the fact that it is likely that WBEM is incorporated in next-generation operating systems.

WBEM is a set of Internet standards-based specifications that define a common management environment leveraging the Web technologies. The WBEM core set of specifications includes:

- a reference data model, i.e. the Common Information Model (CIM);
- an encoding specification, i.e. the xmlCIM Encoding Specification;
- a transport mechanism, i.e. CIM Operations over HTTP.

The CIM specification provides a methodology and language for describing management data in a platform-independent manner, enabling multi-vendor management systems and applications to exchange such data. CIM standard schema is used by applications to describe systems, software objects, networks and devices. CIM enables both 'agent to manager' and 'manager to manager' communications which provides for Distributed System Management. CIM is broken down in the following components:

- The CIM specification – It describes the language, naming, meta-schema and mapping techniques to other management models, especially SNMP MIBs.
- The CIM Meta-Schema – It is a formal definition of the model. It defines the terms used to express the model and their usage and semantics. The elements of the Meta-schema are Classes, Properties, and Methods. The Meta-schema also supports Indications and Associations as types of Classes and References as types of Properties.
- Directory specifications – AS part of the wider DEN (Directory Enabled Networks) standardisation work. DMTF has defined network elements, a service model as well as policy and user management specifications for use in standard directory services that are based on CIM as reference model.

The xmlCIM Encoding Specification defines XML elements, written in Document Type Definition (DTD), that can be used to represent CIM classes and instances. Leveraging XML, CIM allows one to describe information in a universal format and syntax.

The XML/HTTP specification defines a method for transmitting the XML-encoded management information via HTTP.

4.9 Directory Services

In the field of Directory Services, a distinction must be made between two classes of directory services: generic directory services applications, available to the user as specific applications, and 'Built-in' network directory services, which are in fact part of a typical IP network internal apparatus.

4.9.1 Generic Directory Services Applications

Application and operating system software handles a great deal of information on user and resources, providing the means for a user or an application to identify a resource that is needed at any one time and for ensuring that the user only accesses a resource that he/she is entitled to use.

On trans-European networks, the use of standards-based directories is prerequisite to meeting requirements such as:

- ubiquitous access to service information (e.g. access to Certificate Revocation Lists in certification authority services);
- interoperability of services between multivendor platforms and operating systems (e.g. implementation of a single sign-on service for the whole set of independently-supplied applications running on a “common” LocalDomain)
- setting up of policy-driven, centralised operations, etc.

IEFT’s LDAP is the widely supported industry standard for accessing directory services. LDAP is a directory access protocol that defines a simple means of querying data from a directory service platform. LDAP does not address how the directory service itself is structured. It relies on the X.500 model as a proven blueprint for implementing directory services. LDAP is a "lightweight" version of X.500’s DAP (Directory Access Protocol) for use on TCP-based networks.

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the whole directory that is synchronised periodically. An LDAP server is called a Directory System Agent (DSA). An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user.

LDAP v3 also defines a number of improvements to enable client access to the server to be more efficiently implemented and more suitable for the Internet model (e.g. the use of sort keys and paged responses to support type-down addressing). This is essential work, needed to facilitate directory application development and deployment. Importantly, LDAP has so far defined these new functions so that they can be implemented on top of the standard X.500 DAP mechanisms (i.e. without compromising the relationship with X.500).

LDAP is the recommended directory services standard within trans-European networks. Efficiencies and economies are expected to be achieved by having applications, operating systems and users share service data across networks, thus helping planners and managers in avoiding duplication of solutions and achieving massive cost savings. This process cannot be led under a unique procurement policy, though, because trans-European networks are individually planned, funded and implemented, and also because commercial platforms (e.g. databases and operating systems) incorporate bundled, proprietary directory functionality.

As a result, a number of disparate, multivendor directory solutions are and will increasingly be running on existing LocalDomains. Interoperability is, therefore, a key element.

The Open Group and the Directory Interoperability Forum are defining standards and an associated testing and certification framework to deliver interoperability assurance. Interoperability between independent directories is achieved by means of:

- Referrals and Continuation References – when a server to which a request is made does not have all of the requested information, it may return a referral to another server to which the entire request should be directed, or return part of the information together with a continuation reference to another server that can provide the rest.
- Chaining – when a server to which a request is made does not have all of the requested information, it may obtain some of it from another server.
- Replication – information on one server can be copied to others. A particular case of replication is synchronisation of a smaller directory with a larger one.

Currently the above models are supported in commercial products as follows:

- IETF has defined the LDAP protocol for directory access, with native support for chaining. IETF is presently working on protocols for replication and synchronisation;
- Some commercial platforms implement chaining and replication protocols as specified within the X.500 recommendations.

A common solution to ensure directory interoperability is offered by meta directory facilities, offered by commercial platforms. These refer to an LDAP-based master directory containing a superset of the information in all the directories concerned (called slave directories). If a common schema is enforced across all slave directories, the attributes for an object will be the same in all directories. Commonly, commercial software supports functionality that includes:

- feeding of the master directory from existing (slave) directories;
- synchronisation functions towards the master, that are triggered when an event such as object add, update or delete occurs on one of the underlying directories;
- synchronisation functions towards the slaves, that are triggered when an object is added to the master directory or when an update that occurs in a slave directory is propagated to the master directory.

DSML is an increasingly popular way for applications to exchange directory information using XML. DSML enables XML-based applications to use directory information from, and exchange directory information with, other XML-based applications regardless of the specific directories at the remote sites. Applications utilise profile and resource information from directories in their native environment. Using the standard DSML schema, profile and resource information is rendered when needed in XML documents that are sent to other DSML-enabled applications. This effectively extends LDAP across firewalls and to any Internet transport protocol.

Prerequisite to directory interoperability is that the directories share a unique view of the managed objects. To this respect, a directory schema is a key component of a directory architecture. Major developments in this area are underway for directory interoperability as part of the DSML standardisation work, that leverages the standard CIM model (see above, management services.)

From the operational and management point of view, the set of standards known as DEN sets out a suitable framework to define and enforce a directory-based networking policy. The Directory Enabled Network (DEN) initiative and related specification work carried out by the Distributed Management Task Force (DMTF) is an effort to build intelligent networks and networked applications that can associate users and applications to services available from the network, according to a consistent set of policies.

Drawing on the CIM standards, DEN defines a standard information model and schema for independent actors to provide end-to-end services. In a trans-European network scenario, when a user asks for a service, that service must be delivered in an end-to-end fashion across multiple networks. DEN is a template for exchanging information that enables all the service providers concerned to share a common definition of the service, although each of them implement their service in their own way. DEN defines a directory as a centralised repository that co-ordinates information storage and retrieval.

Enforced via XML, the DEN schema enables a coherent distributed system management framework. As part of the overall framework, DEN's standardised directory schema defines managed elements in a system and network. This schema specifies physical objects such as computer systems, software objects, devices, etc. DEN can then be used as a conceptual information model for describing management that is not bound to a particular implementation.

As part of the IDA programme, work is underway to define a common trans-European network schema to facilitate separate directories' integration. The initiative, called IntDir will deliver:

- Directory Interoperability: specific schema recommendations that determine what can be stored in a directory in order to ensure the integrity and quality of data, and to establish and ensure an interoperability framework.
- Namespace considerations, which provide the means by which directory data is named and referenced.
- Access Management Guidelines and recommendations, which indicate how IDA can provide a complete integrated security infrastructure (part of its middleware tier) for applications that includes authentication, authorisation and a common administration/development framework.

4.9.2 Built-in Network Directory Services

'Built-in' network directory services in an IP network provide the possibility of defining and maintaining mapping tables between the IP addresses of the recipient and the recipient Domain Names.

Domain Names are used within the IP network to define logical domains, where an organisation is fully responsible for the administration of the set of users located inside that domain. Such 'built-in' directory features are called Domain Name Services. They provide end-users with the possibility of reaching the recipient domain by typing the domain name instead of the IP address.

Domain Name services are provided on a de facto basis, since they are embedded and intervene as an active component for routing IP packets.

4.9.3 Secure DNS Implementation

Some additional concerns about DNS security must be discussed. Indeed, the DNS implementation is the heart of routing within an IP network.

A secure end-to-end DNS implementation is closely linked to the implementation of firewalls at the boundary of responsibility domains, and is definitely a major topic within the SLA on security, when implementing:

- An IP connection between the LocalDomain and the EuroDomain;
- An IP connection between the EuroDomain and any other domain providing a gateway to application services.

5 Roadmap from Requirements to Application Implementation

5.1 Introduction

This chapter helps you to select a solution outline, including its associated service profiles, based on a number business requirements and issues. The selection process that is provided here consists of the following steps:

- Locate your relevant business requirement in the table of requirement categories (see paragraph 5.2.1) and consult the section with business issues, in particular the security issues (see paragraph 5.2.2).
- Consult the table with the relevant requirement category (see paragraphs 5.2.3 – 5.2.8). Each of the tables comprises the following information sets:

Type of process and type of content	This information helps you to identify a particular process within the business requirement category.
Mechanism description and security requirement class	This information provides an outline of the solution that matches the selected requirement.
Services	This information shows the components of the solution outline in terms of types of services and service profiles. This information shows the components of the solution outline in terms of types of services and service profiles. Services are specified in terms of their location onto the elements of a trans-European network, covering: • a client part – services that run on the client workstation; • a user LocalDomain – services that run on the network of the partner organisations; • a Common LocalDomain – software that runs on a particular LocalDomain to provide a centralised service (e.g. giving access to a common database) to user LocalDomains.
Security	This information shows the security services and service profiles related to the relevant security requirement class. Use of PKI services is assumed whenever protocols such as S-Mime and SSL are recommended.

- Consult the diagram in paragraph 5.3 for a graphical representation of the various solutions, within the context of the entire architecture.
- Consult chapter 2 of the Annexes, Service Profiles, for more details on each of the Service Profiles referred to in the tables and diagram.

5.2 Business Requirements and Issues

5.2.1 Business Requirements

General requirement context and outline	Category
Processes in which relevant data is gathered from distributed sources (i.e. multiple LocalDomains) potentially across all the EU into a common EU database (hosted on a LocalDomain belonging to a coordinating organisation e.g. by Commission, Agencies, etc.). This model is suitable when a central organisation is responsible for, or is simply willing to provide, support or coordination services.	Data collection, see Category 1
Processes that involve relevant data being mutually exchanged between two users/applications on two LocalDomains. This model is frequently used, especially when legislation attaches particular importance to the exchange itself (i.e. formal notifications) but also because it preserves independence of the counterparts that only need to agree upon an EDI-type exchange format and to set up a translation/conversion process on their existing application systems.	Data exchange, see Category 2
Processes in which relevant data is centrally stored; data is accessed from distributed points by query/answer processes. This model provides both a counterpart to the data exchange model, but is also increasingly used as an alternative to data exchange using interactive means (partner systems expose light client-based interface to counterparts e.g. XML or Java-based).	Data dissemination, Category 3
Processes in which data needs to be shared in order to allow several departments or persons to collaborate in the activities to be performed on the data.	Data sharing, see Category 4
Requirements for sending notifications that imply a reply within a defined time scale and a common context between users (security, authentication, etc). This requirement may be associated to one of the communication models described above.	Alerts, see Category 5
Service processes, supplementary to all others.	Services, see Category 6

5.2.2 Business issues

In selecting a solution, the following business issues need to be taken into account.

- Timeliness, period within which a required result must have been obtained, or an action must have been performed. This marks the difference between a requirement for data exchange/collection and data sharing.
- Legal issues, e.g. obligation to deliver particular data influencing the type of contents to be handled and the communication mechanism chosen.
- Security. Two levels of security requirements are addressed: normal and high. Security requirements are dependent upon the risk that an information confidentiality, integrity and availability breach occurs, to be determined on a case-by-case basis via risk analysis. For the purposes of the roadmap, the following simplified classification is used:

Normal The security risk involved is low to medium. This is the case when an information confidentiality or integrity breach would cause little harm, or when the threat level that system resources are exposed to is low (examples: there is little interest of third parties to get hold of the information; only a restricted number of well trained people are designated to use the system; the information handled is widely available, etc.)

High The security risk involved is significant. This situation occurs when an information confidentiality or integrity breach would cause significant harm (e.g. disclosure of sensitive information), or because the threat level that system resources are exposed to is high (e.g. the system serves a large, heterogeneous user community on the Internet; etc.)

Please note that to simplify roadmap options, availability is assumed to affect more the sizing of a system then its functional architecture. As a consequence, it is assumed that a project would handle higher availability requirements by cloning or replicating front-end systems (e.g. Web cluster), coupled with a stateless load-balancing function, and partitioning the online content across multiple, redundant, raid technology-based back-end systems.

In accordance with the definitions of CD 95/86/EC, applications that handle sensitive personal data should always be regarded as involving security requirements level high.

Particular attention should be paid to the Council Decision 2001/264/EC adopting the Council's security regulation and the Commission Decision 2001/844/EC on the Commission Provision on Security, which set out legal provisions on how to treat classified information.

The above classifications only covers non-classified information, i.e. information and material that can be treated with normally prevailing security measures because it does not affect interests of the European Union or of one or more of its Member States.

Information categories referred to by law as "EU RESTRICTED", EU CONFIDENTIAL, EU SECRET and EU TOP-SECRECT can only be handled by accredited systems that support the so called ***mandatory access control***. Such requirements are outside the scope of these guidelines and are to be dealt with on a case-by-case basis.

5.2.3 Use of generic services and common tools

Often, requirements identified in the roadmaps can be met by IDA tools and techniques available to all trans-European projects.

Generic services

The following list shows the generic services that are available to date:

Generic service	Usage	Reference to requirement category
TESTA	Use of TESTA II is encouraged for all requirement categories, except when the following requirements occur: • communication with users not belonging to the established community; • requirements for mobility.	All requirements categories, especially those with Security class set to high
CIRCA	CIRCA is a web-based environment that offers a common virtual space for work-groups and networks, enabling the effective and secure sharing of resources and documents.	Data exchange and data sharing
PKICUG	Use PKI services for all categories if security class is high. On a case-by-case basis, if TESTA is used by all users, extra security measures such as SSL encryption may be required.	All requirements categories where SSL and/or S-Mime apply

Common tools

The following list shows the common tools that are available to date:

Area	Tools and techniques	Description	Data exchange	Data collection	Data dissemin.	Data sharing	Alert system
Application services	CIRCA	Web-based environment offering a common virtual space for work-groups and networks, enabling the effective and secure sharing of resources and documents.	X			X	
	IDA-QA	Quality programme aimed at facilitating the achievement of business needs in trans-European projects by defining QA guidelines and generic self-assessment tools.	X	X	X	X	X
Data content interoperability	MoReq	Comprehensive specification of functional requirements for the management of electronic records.	X			X	
Front Office	Portal toolkit	Web-based gateways to information on Internet, business-to-business, and corporate environments maintained by content-provider communities.			X		
Back Office	STATEL	An API library and a command interface offering a transparent service for bi-directional file transfer.	X	X			
Software	Use of Open Source software	Information about the use of open source software in public administrations	X	X	X	X	X

Use of these tools, when appropriate to the business requirements at hand, is strongly encouraged.

Currently, new tools are being developed and others are being evaluated as candidate tools. Further information may be found at the following address: http://europa.eu.int/ISPO/ida/ida.htm.

Disclaimer

Please note that the solutions illustrated in the following tables are based on best practice considerations. The information on security is temporary since the Commission's security policy is under review.

The solutions provided are not mandatory. However, the tables help the reader to make choices based on the underlying architecture principles as set out in these guidelines.

.

5.2.4 Requirement category 1, Data collection

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Authentication, Access control	Consistency, integrity	Confidentiality	Non-repudiation
1.1	**Transfer of data held by the sender in electronic format**	Business documents held by the sender either revisable (Office) or non-revisable (PDF) to be centrally collected	A file is uploaded to a centralised repository via a webservice (Web post)	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		Webserver Document management system or simple file system	User-ID & Password-based authentication and authorisation on Common Local Domain			
1.2				High	same as above	same as above	same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	
1.3			Sending as an attachment to e-mail files for storage on a centralised repository	Normal	e-mail client	e-mail account	Mail server Application to process and store incoming files Send automated acknowledgement				
1.4				High	same as above	same as above	same as above		S-Mime	S-Mime	S-Mime
1.5		Structured data between processes	Application to application (data is processed locally and converted to an agreed business message)	Normal	Dependent on technology used locally	EbXML, SOAP implemented on technology platform of the sender organisation	SOAP, JTS for transaction management, JSP for message transformation, EJB, JSP, JDBC RDBMS				
1.6				High	same as above	same as above	same as above	XML signature	SSL	SSL	XML signature
1.7	**Transfer of data that is not available in electronic format**	Structured data to be fed to a Common LocalDomain	A web-based forms-type transactional application is used to collect data	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		Webserver Application server Servlet, EJB, JSP, JDBC RDBMS	User-ID & Password on Common Local Domain			
1.8				High	same as above	same as above	same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature

5.2.5 Requirement category 2, Data exchange

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Authentication, Access control	Consistency, integrity	Confidentiality	Non-repudiation
2.1	**Initiated by the sender**	Data on business documents held by the sender either revisable (Office) or non-revisable (PDF) to be sent to peer LocalDomain	Direct e-mail between LocalDomains Option: notary service	Normal	e-mail client	e-mail account	Optional: Notary service (ref)				
2.2				High	same as above	same as above	same as above	S-Mime	S-Mime	S-Mime	S-Mime
2.3			Direct Web post to counterpart LocalDomain	Normal	Browser	on the recipient's LocalDomain: - Website - Document management system or simple file system	Optional: Notary service (ref)	User-ID & Password-based Authentication and authorisation			
2.4				High	same as above	same as above	same as above	User-ID & Password on counterpart LocalDomain SSL authentication	Signed Java SSL	SSL	XML Signature
2.5			Web post to a centralised message routing service	Normal	Browser		Webserver Doc. management system or simple file system Application for message management and routing, delivering as in 2.9 or 2.11	User-ID & Password			
2.6				High	same as above	same as above	same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature
2.7		Structured data to be fed to a central notification management system	A web form-based transactional application is used to collect notification data	Normal	Browser (XML, HTML, XSLT, DOM, Applets)	--	Webserver, Application server, Servlet, EJB, JSP, JDBC, RDBMS Application for message management and routing, delivering as in 2.9 or 3.3	User-ID & Password on Common Local Domain			
2.8				High	same as above	same as above	same as above	User-ID & Password on Common Local Domain SSL authent.	Signed Java SSL	SSL	XML Signature
2.9		Structured data between processes	Appl. to appl. (data processed locally and converted to agreed business message)	Normal	Dependent on technology used locally	EbXML, SOAP implemented on platform of partner org.	Optional: Notary service (ref)				
2.10				High	same as above	same as above	same as above	XML signature	SSL	SSL	XML signature
2.11	**Initiated by the recipient**	Generic document	Download data from website / post box		Browser	Website for message management	--	Encryption, PKI		Authentication and authorisation onto webserver SSL, User-ID Password	SSL

5.2.6 Requirement category 3, Data dissemination

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Authentication, Access control	Consistency, integrity	Confidentiality	Non-repudiation
3.1	**Push-based, initiated by the sending body**	Unstructured and structured data	Send as an attachment to e-mail addressed to mailing lists	Normal	e-mail client	e-mail account	Application to send automated e-mail, or User-made e-mail				
3.2				High	Same as above	Same as above	Same as above	S-Mime	S-Mime	S-Mime	
3.3			Internet publishing – Centralised Portal with high customisation (customised "what's new" sections to be assembled "on-the-fly" presented individually to users upon logon)	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		Web portal with user profiling – Functionality includes capability for administrators and users to tailor services upon user profiles	User-ID & Password			
3.4				High	Same as above	Same as above	Same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature
3.5	**Pull-based, on demand from recipient requests for files or subjects that are known to be present**	Unstructured and structured data	Connect & retrieve from: - Web-enabled document management system Or - Web-enabled repositories	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		- Application to manage documents, organised in "folders" (topics areas) via navigation capability, or - Application menus for access to form-based information	User-ID & Password			
3.6				High	Same as above	Same as above	Same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature
3.7	**Search-based, information that may be present or not**	Unstructured and structured data	Search engines & Indexing engines	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		Application to send XML-based query form to user and to return: - a result list - specific form	User-ID & Password			
3.8				High	Same as above	Same as above	Same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature

5.2.7 Requirement category 4, Data sharing

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Authentication, Access control	Consistency, integrity	Confidentiality	Non-repudiation
4.1	**Access to shared areas for co-authoring**	Structured XML documents for collaborative editing, plus communication frame for online communication	Connect to web-based collaborative environment & retrieve: - document structure -text objects - multimedia Capability to upload and attach locally-edited components to XML document	High	Browser (XML, HTML, XSLT, DOM, Applets)		- Application to manage documents, organised in "folders" (topics areas) via navigation capability, or - Application menus for access to form-based information	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature
4.2	**Search-based, information that may be present or not**	Structured XML documents for collaborative editing	Search engines & Indexing engines	High	Browser (XML, HTML, XSLT, DOM, Applets)		Collaborative environment to send XML-based query form to user and to return a result list on: - documents; - revisions; -related documents - etc.	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature

5.2.8 Requirement category 5, Alerts

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Confidentiality	Consistency, integrity	Authenticity, Access control	Non-repudiation
5.1	**Push-type, urgency moderate**	e-mail-based alert message	E-mail an agreed structured message, digitally signed by sender	High	e-mail client	e-mail account	Optional: See notary service (ref)	SMIME		SMIME	Digital sign.
5.2	**Push-type, urgency high**	Interrupt-based alert message	Agent placed on desktop via JVM	High	JVM			User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature
5.2	**Pull-type, urgency moderate**	Document-based information	Internet publishing – Centralised Portal with high customisation (customised "what's new" sections to be assembled "on-the-fly" presented individually to users upon logon)	Normal	Browser (XML, HTML, XSLT, DOM, Applets)		Web portal with user profiling – Functionality includes capability for administrators and users to tailor services upon user profiles	User-ID & Password			
5.4				High	same as above	same as above	same as above	User-ID & Password on Common Local Domain SSL authentication	Signed Java SSL	SSL	XML Signature

5.2.9 Requirement category 6, Service process

Ref.	Type of process	Type of content	Mechanism description	Security Req. Class	Services			Security			
					Client	User Local Domain	Common Local Domain	Authentication, Access control	Consistency, integrity	Confidentiality	Non-repudiation
6.1	**Acknowled-gement**	Notification message, returned by the recipient of a data exchange to the sender	E-mail an agreed structured message, digitally signed by sender	High	e-mail client	e-mail account		SMIME		SMIME	Digital sign.
6.2	**Notary**	Notification message, to be sent by a user who carries out a transaction to a central notary system	E-mail an agreed structured message, digitally signed by sender	High	e-mail client	e-mail account	e-mail based repository	SMIME	=	SMIME	Digital sign.

5.3 Diagram

The diagram on the following page provides a high-level view of the trans-European network application models and the building blocks concerned. The diagram emphasises the services used by the various application types and how the building blocks interoperate across different LocalDomains.

To present the alternatives, various LocalDomain configurations are presented as follows:

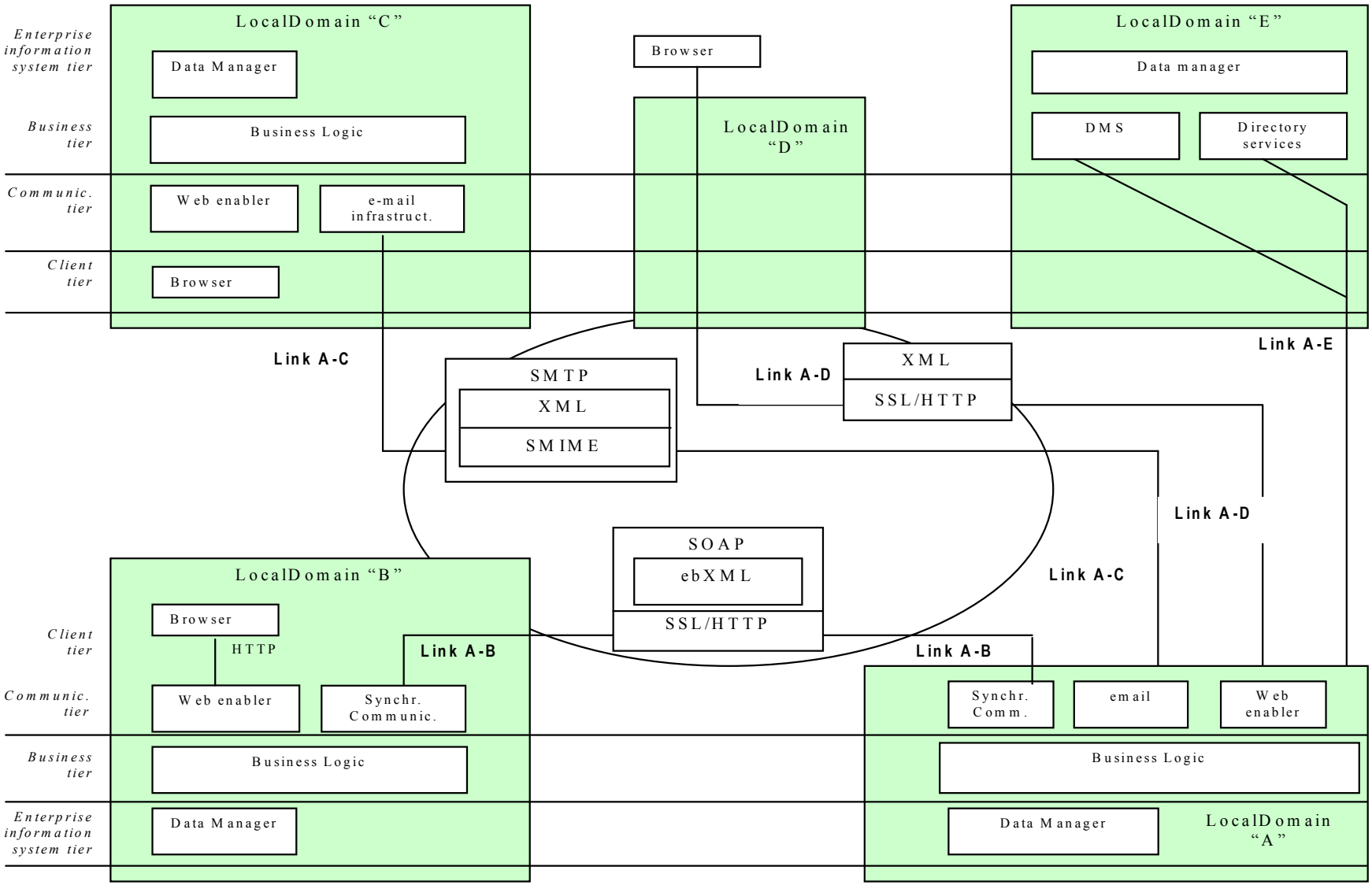
- LocalDomain "A" runs a business application serving "client" LocalDomains. It maintains a centralised database with all information relating to exchange of business documents between EU organisations. This situation occurs when an EU organisation is responsible for the provision to counterpart organisations in the MSs of a given service as part of a business process. LocalDomain "A" operates as follows:
  - Over the link A-B, it enables document exchanges with counterpart LocalDomain "B" using ebXML and SOAP. (See requirement type "**data exchange**" in the roadmap.)
  - Over the link A-C, it enables document exchanges with counterpart LocalDomain "C" using XML over an e-mail infrastructure. In this case, customised software must be in place on both LocalDomains to provide translation/conversion functionality, plus process management. (See requirement type "**data exchange**" in the roadmap.)
  - Over the link A-D, it enables document exchanges with counterpart LocalDomain "D" using XML over an interactive, web-enabled infrastructure. Probably, LocalDomain "A" offers a message management environment to LocalDomains that do not have their own system to process and manage the required information. (see requirement type "**data collection**" and "**data dissemination**" in the roadmap.)
- Over the link A-E, LocalDomain "A" accesses generic services and common tools over the IDA infrastructure, such as Directory services, authentication services, document management services (e.g. CIRCA)

- The LocalDomain "B" system processes data independently. As soon as it has to make a notification, it runs an ebXML-enabled application that extracts data from the internal database, maps it on to the relevant SOAP message and sends it to the business partner "A".

- The LocalDomain "C" system also processes data independently, yet it runs a custom application that extracts data from the internal database and maps it on to the relevant XML schema. Then another application takes over to perform the exchange over the email infrastructure and stores tracking and tracing information on the events.

- Users on LocalDomain "D" just use a common web browser. With this tool, they have access to a management facility offered by LocalDomain "A" handling the business information exchange. There is no message management whatsoever on LocalDomain "D". Probably, LocalDomain "A" provides extensive functionality to process data and to query the database.

Please note that the capability for the user at LocalDomain "D" to query the centralised database using a web browser is available to all other LocalDomains.


Enterprise information system tier
Business tier
Communic. tier
Client tier
LocalDomain "C"
Data Manager
Business Logic
Web enabler
e-mail infrastruct.
Browser
Browser
LocalDomain "D"
LocalDomain "E"
Data manager
DMS
Directory services
Link A-C
Link A-E
Link A-D
SMTP
XML
SMIME
XML
SSL/HTTP
SOAP
ebXML
SSL/HTTP
Link A-C
Link A-D
LocalDomain "B"
Browser
HTTP
Link A-B
Link A-B
Web enabler
Synchr. Communic.
Business Logic
Data Manager
Synchr. Comm.
email
Web enabler
Business Logic
Data Manager
LocalDomain "A"