ARCHITECTURE GUIDELINES

For Trans-European Telematics Networks for Administrations

Version 7.1
## Contents

1 EXECUTIVE SUMMARY ................................................................. 3
  1.1 MISSION STATEMENT ................................................................. 3
  1.2 DOCUMENT STRUCTURE ............................................................ 3
  1.3 PROPRIETARY PRODUCTS .......................................................... 3

2 SURVEY OF USER REQUIREMENTS .............................................. 5
  2.1 INTRODUCTION ........................................................................... 5
  2.2 FUNDAMENTAL REQUIREMENTS ................................................. 5
  2.3 GENERIC BUSINESS REQUIREMENTS ........................................... 5
  2.4 SECURITY REQUIREMENTS ......................................................... 7
  2.5 IMPLEMENTATION REQUIREMENTS ............................................ 7
    2.5.1 Helpdesk and Support Functions ............................................. 8
    2.5.2 Network Management and Administration Services .................. 8
    2.5.3 Directory Services ............................................................... 8
  2.6 ADDITIONAL REQUIREMENTS .................................................... 8
    2.6.1 Requirements for disabled persons ......................................... 8

3 IMPLEMENTATION PRINCIPLES .................................................. 9
  3.1 INTRODUCTION ........................................................................... 9
  3.2 SUBSIDIARITY ............................................................................ 9
  3.3 SECURITY POLICIES ................................................................ 9
  3.4 MULTILATERAL SOLUTIONS AND AGREEMENTS ......................... 9
  3.5 OPEN STANDARDS .................................................................... 9
  3.6 OPEN SOURCE SOFTWARE ....................................................... 10
  3.7 GENERIC SERVICES AND COMMON TOOLS ............................... 10

4 IMPLEMENTATION APPROACH ................................................... 12
  4.1 INTRODUCTION .......................................................................... 12
  4.2 INTERCONNECTION SERVICES .................................................. 13
    4.2.1 Reference networking model ................................................... 13
    4.2.2 Domain Name Services .......................................................... 15
    4.2.3 Identity Management Services ............................................... 16
    4.2.4 Additional Services ............................................................... 17
  4.3 DATA INTEGRATION AND MIDDLEWARE .................................. 20
    4.3.1 Application models ............................................................... 20
    4.3.2 Content interoperability .......................................................... 20
    4.3.3 Technologies ....................................................................... 20
  4.4 DATA PRESENTATION AND EXCHANGE .................................. 22
    4.4.1 Services and tools ................................................................. 22
  4.5 SECURITY SERVICES .............................................................. 23
    4.5.1 Information System security implementation ............................ 24
    4.5.2 Application security scope ..................................................... 24
    4.5.3 A PKI for trans-European projects ...................................... 25

5 ROADMAP FROM REQUIREMENTS TO APPLICATION IMPLEMENTATION 27
  5.1 INTRODUCTION .......................................................................... 27
  5.2 BUSINESS REQUIREMENTS AND ISSUES ................................. 28
    5.2.1 Business Requirements .......................................................... 28
    5.2.2 Business issues .................................................................... 28
    5.2.3 Use of generic services and common tools ............................... 29
    5.2.4 Requirement category 1, Data collection ................................ 31
    5.2.5 Requirement category 2, Data exchange .................................. 32
    5.2.6 Requirement category 3, Data dissemination ............................ 33
    5.2.7 Requirement category 4, Data sharing .................................... 34
    5.2.8 Requirement category 5, Alerts .............................................. 35
    5.2.9 Requirement category 6, Service process ............................... 36
  5.3 DIAGRAM .................................................................................. 37
LIST OF FIGURES
Figure 1, Basic components of the IDA Architecture............................................................12
Figure 2, Private and public networking solutions..............................................................13
Figure 3, IS security implementation..................................................................................24
Figure 4, Interoperability between LocalDomains.............................................................38

HISTORY OF DOCUMENT

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 4.1</td>
<td>01/03/1999</td>
<td>First draft based on V.3.2.1 extended by a new chapter on IPNET (derived from the IPNET document V2.2.c).</td>
</tr>
<tr>
<td>Version 5.0</td>
<td>31/08/2000</td>
<td>Update of version 4.1, with improved structure and updated and extended information on new technologies.</td>
</tr>
<tr>
<td>Version 5.1</td>
<td>29/09/2000</td>
<td>Update of version 5.0, after processing review comments forwarded by the Commission.</td>
</tr>
<tr>
<td>Version 5.2</td>
<td>12/10/2000</td>
<td>Update of version 5.1, after processing review comments forwarded by the Commission’s PAB.</td>
</tr>
<tr>
<td>Version 5.3</td>
<td>12/02/2001</td>
<td>Update of version 5.2, after processing review comments forwarded by the TAC.</td>
</tr>
<tr>
<td>Version 6.0</td>
<td>31/08/2001</td>
<td>Update of version 5.3, with roadmaps and updated and extended information on new technologies.</td>
</tr>
<tr>
<td>Version 6.1</td>
<td>21/06/2002</td>
<td>Update of version 6.0, after processing review comments forwarded by the TAC WHAM.</td>
</tr>
<tr>
<td>Version 7.0</td>
<td>04/11/2002</td>
<td>Update of first draft of version 7.0, after processing review comments forwarded by the Commission’s PAB.</td>
</tr>
<tr>
<td>Version 7.1</td>
<td>13/02/2004</td>
<td>Update of version 7.0.</td>
</tr>
</tbody>
</table>
1 Executive Summary

1.1 Mission Statement

These Guidelines describe an architecture agreed upon by the IDA (Interchange of Data between Administrations) community that enables trans-European networks to interoperate, and thus allows 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.

The Architecture 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 generic services and common tools as soon as these are made available by the IDA and IDABC programmes to the EU user community.

The direct benefits of having a clearly defined architecture comprise:

- improved inter-operability between the IT and networks systems of business partners;
- 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 access the trans-European Services, or as a technical framework for the achievement of generic services. Using IDA and IDABC generic services on a common architecture will:

- reduce costs thanks to reusability and economy of scale;
- shorten the implementation time of new projects;
- improve manageability of projects and of the implemented solutions;
- set a clear migration path for existing, heterogeneous projects;
- leave Administrations to concentrate on their core business applications.

1.2 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 implemented 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.

The Annexes contain 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 these architecture guidelines.

1.3 Proprietary Products

All care has been taken to ensure that the text of these Guidelines does not make any reference to proprietary products. However, if the text does contain any explicit or implicit reference to any proprietary product, this does not 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 put forward 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 generic services and 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’ Administrations (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 Member States 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 the 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 (i.e. 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). It should 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** 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 a 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 implemented 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 Web Content Accessibility Guidelines, please refer to section 2.5 of the Annexes to this document. The Annexes also provide information on the SPRITE-S² project ACCENT, which addresses the issue of accessibility in public ICT procurements.
3 Implementation Principles

3.1 Introduction
Adherence to the IDA architecture requires compliance with the principles described in this chapter. The following chapter - Implementation Approach - describes a range of solutions that are based on these principles. For additional information and a description of future trends please also refer to the European Interoperability Framework available at the IDABC website\(^1\).

3.2 Subsidiarity
A basic principle of the IDA(BC) architecture is the autonomy of the business partners that make use of the internetworking architecture. While business partners exchange or share information, they must be able to choose their own policies and practices (i.e. technological approach, legal framework, principles of management, etc.).

The internetworking model of the IDA(BC) architecture offers and safeguards this autonomy by means of separation between a central, common infrastructure, the EuroDomain or Internet, and the local networks of the business partners, the LocalDomains. Access to the common infrastructure is offered by network interfaces called EuroGates or by Internet Service Providers.

3.3 Security policies
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.

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.

3.4 Multilateral solutions and agreements
Interoperability partners are invited to establish collaboration agreements and develop common solutions in those projects in which they exchange data. They should avoid the implementation of bilateral arrangements as this will create the need for the maintenance of a multitude of solutions and agreements. Instead, they should opt for multilateral solutions that provide the benefit of developments that are done once and are available to all parties. Apart from elements of particular significance for the applications in question, agreements and solutions should establish minimum requirements of operational significance, such as opening hours, software version control, troubleshooting arrangements, etc. Moreover, if needed, charging policies should be defined at the project planning stage and included in contacts and agreements.

3.5 Open Standards
The use of Open Standards\(^2\) is encouraged and adopted as much as possible. Open Standards are not just specifications but have some important characteristics. They are available to all to read and implement and in this way, create competition and help in avoiding vendor-specific implementations. Open Standards and the organizations that administer them do not favour one implementer over another and provide the Standards for free for all to implement, with no royalty or fee.

\(^1\) http://europa.eu.int/ida/en/document/2319
\(^2\) for a definition see The European Interoperability Guidelines (EIF), http://europa.eu.int/ida/en/document/2319
3.6 Open Source Software

The use of Open Source Software (OSS) should also be assessed and promoted, especially in cases where it provides alternatives to proprietary solutions. OSS products are publicly available and the availability of their source code provides fertile ground to the making of more robust and interoperable specifications.

3.7 Generic services and common tools

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.

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 Introduction

This chapter describes the architectural models and the services and standards that constitute the heart of the IDA Architecture Interoperability model. The design of this architecture and the selection of its underlying models and components:

- addresses the various user requirements as described in chapter 2, e.g. autonomy of business partners, ample security facilities and the use of open standards;
- are governed by the implementation principles as stated in chapter 3, e.g. maximum use of generic services and common tools and a maximum degree of reusability.

Each section presents the relevant services or service models that cover the current approach to solutions for a particular service. Subsequently, each section describes the enabling technologies that can be employed for the implementation of the service.

In general, the IDA Architecture is based on the following conceptual diagram:
4.2 Interconnection Services

4.2.1 Reference networking model
Internetworking services between LocalDomains are built on top of the IP generic standards. The choice of internetworking services and service levels to be implemented 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 public route, i.e. the Internet.

![Figure 2, Private and public networking solutions](image)

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

The EuroDomain consists of:
- a common internetworking platform, in terms of requirements, specifications and functionality for trans-European information services;
- a set of interface definitions (protocols, formats, APIs) for the backbone infrastructure of trans-European telematics applications;
- services that implement these features, including exhaustive functional and technical documentation.

To ensure technical independence between the EuroDomain and the LocalDomains, the EuroDomain is not directly accessible. Instead, a pair of EuroGates provides the connectivity and interoperability between any two LocalDomains via the EuroDomain (and to the EuroDomain services themselves).
EuroDomain services are based on specifications and service level agreements that are agreed upon by the IDA community. As part of the IDA(BC) responsibility to assist EU organisations with the setting up of trans-European networks, a number of EuroDomain services (including VPN services) are offered within the IDA and IDABC programmes. The actual services themselves are entrusted to service providers after centralised procurement through public procedures.

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

**EuroGate**

The separation of responsibility between the EuroDomain and LocalDomains is achieved through an access point called “EuroGate”. The EuroGate is a key architecture element that provides both flexibility and the managerial and technical independence between the Domains. It should not be seen as a particular machine, computer or gateway device. Instead, the EuroGate is a set of interface services that ensure interoperation between LocalDomains in such a way that roles and responsibilities for domain administration (both Local and Central) remain separate.

A EuroGate’s functionality includes access routing to the EuroDomain network, security (encryption), identity management, accounting and charging, network management, etc., and even the protocol conversions (e.g. EDI-XML) that may be necessary for interoperation between legacy systems.

A EuroGate may be designed to serve one or multiple organisations.

EuroGate management and administration responsibilities may rest with either the organisation responsible for the infrastructure of the business partner(s) within a given LocalDomain, or with the EuroDomain manager, or be shared by both, based on service level agreements set out within the IDA programme.

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.

**LocalDomains**

A LocalDomain consists of people, resources, information and communication technology equipment as well as the infrastructure, information and data related with a specific set of business processes of a partner organisation.

A LocalDomain may also be seen as a set of services available to a plurality of business partner, for organisations that pool together on account of common business and/or operational requirements. Therefore, a single EuroGate may link individual networks (e.g. LocalDomain “A” and “B” in the figure above) but also networks of networks (e.g. LocalDomain “C” in the figure above) used by partner organisations.

Each Member State may have its agencies 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.

A National Agency may wish to set up its own EuroGate, while similar organisations within a Member State may pool together and connect to the EuroDomain by means of only one EuroGate. In some application scenarios, LocalDomains may each be so small that it is more cost-effective to share a EuroGate for their connection to the EuroDomain. This also occurs when a National Network is linking National Administrations, and only one EuroGate is available as gateway to the EuroDomain for these Administrations.

In all such cases, a LocalDomain is managed and controlled by the organisation that owns 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. External services can also consist of services provided on the Internet.
However, if a LocalDomain wishes to set up connections to the Internet, it is important to realise that direct access to the Internet from the EuroDomain backbone is prohibited. Internet connections must, therefore, be implemented within a LocalDomain. At the same time a security policy must be defined that needs to be notified to all trans-European project partners and stipulated in the co-operation agreement.

**TESTA II**

TESTA offers European administrations a telecommunications interconnection platform and services that enable the exchange of data between administrations while guaranteeing performance, availability and security to a degree not available through other communication networks.

The TESTA infrastructure is in conformance with the model of the EuroDomain and the LocalDomains as defined in the IDA Architecture Guidelines. It offers 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 European backbone network – the EuroDomain – is provided by a telecommunications operator.

The TESTA service suite:

- is dedicated to trans-European communications of the public sector and provides access to the highest number of European administrations of any private network;
- operates at speeds that make it capable of accommodating real-time applications;
- protects local domain security by systematically using network address translation at each access point;
- operates on a clear IP addressing plan structured by geography and operates on a dedicated range of addresses that are not Internet-routable;
- has in-built redundant routing and is governed by availability guarantees, network monitoring and security incident intervention capabilities are in place;
- will provide information confidentiality through the introduction of encryption and other protective measures, both on the level of the backbone network and at local levels;
- encourages network service integration with other IDA services, such as IDA’s public key infrastructure (PKICuG) and workgroup support tool (CIRCA);
- is managed by one contractual responsibility: IDA.

TESTA also provides network-related application services, such as:

- Domain Name Services
- E-mail relay
- Information gateways

**Internet**

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 Internet Service Provider (ISP). Disadvantages of its use have mainly to do with performance (reliability, response times etc) and the need for additional mechanisms when security is a consideration.

**4.2.2 Domain Name Services**

Domain Names Services (DNS) are ‘built-in’ directory features 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. DNS provides the ability of reaching a counterpart domain by means of a domain name instead of an IP address, by defining and maintaining mapping tables between the IP addresses Domain Names in a network.
A secure end-to-end DNS implementation requires the implementation of firewalls at the boundary of responsibility domains, and is definitely a major topic within a SLA on security between trans-European network partners, when implementing:

• an IP connection between the LocalDomain and the EuroDomain/Internet;
• an IP connection between the EuroDomain/Internet and any other domain providing a gateway to application services.

4.2.3 Identity Management Services

Reference identity management model
IDA trans-European projects should include a sound, directory-based, identity management framework.

Directories fill several roles supporting and integrating the top-tier systems. Directories hold information on users and user profiles, forming the basis for user authentication and authorisation. Policy-based management systems use the directory to reduce the costs of managing desktop computers, network devices and other systems. They also increase network efficiency, allowing managers to personalise the network to fit the needs of individuals, groups, and applications.

All these abilities are collectively referred to as identity management.

Identity management includes three major functions: identity administration, community management, and identity integration.

• Identity administration is the provisioning and maintenance of individual identities. In today’s dynamic business, where resources change continuously, identity administration eases activities such as: creating application accounts and access rights, adding e-mail address book entries, installing applications, configuring dial-up connections, assigning a phone number, assigning office space and computer equipment, etc.

• Community management addresses the connection and security of relationships between identities. It is commonly broken down into two distinct functions:
  - Authentication - the process of verifying the identity of each person using an organisation’s computing infrastructure. Because people are granted access to company resources based on their identities, it is important that individual identity be verified in order to protect privacy and ensure security of the company’s computer systems.
  - Authorisation - the process of granting access to resources based on the credentials of a person’s identity and context. The function passes access credentials of an authenticated user to the system resources to provide access control

• Identity integration focuses on the connection and cooperation of multiple identity repositories based on business rules.

Identity management technology
IEFT’s LDAP (Lightweight Directory Access Protocol) 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.

To achieve interoperability between directories of trans-European network partners, IDA is considering several aspects:

• schema recommendations for directory interoperability 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.
• name space considerations, which provide the means by which directory data is named and referenced.

• access management guidelines and recommendations, which indicate how a complete, integrated security infrastructure (part of a middleware tier) can be provided for applications that includes authentication, authorisation and a common administration/development framework.

Interoperability between directory software is achieved by means of XML-based standards such as DSML. 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 then sent to other DSML-enabled applications. This effectively extends LDAP across firewalls and to any Internet transport protocol.

Finally, a 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 specifications from 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.

4.2.4 Additional Services

The services presented in this section are applicable only in the case of a networking architecture based on the EuroDomain model (Private Network Backbone).

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 in accounting records that form 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.

**Logging**

The EuroDomain and the EuroGates should support common tools and mechanisms for logging EuroDomain service utilisation information. The complete utilisation information 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.
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 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.

Procedures for helpdesk and support services should be defined in service level agreements. Examples of agreements and standard operating procedures that can serve as a model are available for the CIRCA services (http://forum.europa.eu.int).

The Quality Assurance section of the IDABC website provides information on IDABC’s strategy and implementation principles for Quality Assurance and Control, which is intended to improve:

- the manner in which project objectives and requirements are specified;
- the manner in which a project is carried out;
- quality of the project deliverables.

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 or ISP 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.

Technology
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.
4.3 Data Integration and Middleware

4.3.1 Application models
The following two models are commonly implemented in trans-European networks:

- **Transactional model** – A centralised system running on a LocalDomain grants access to individual users at counterpart LocalDomains by means of a web interface. Business partners input, query and retrieve information from the web. The central service runs an SQL-based relational database system if itemised data is concerned and/or a document management system for document-based information.

- **Application-to-application communication model** – Based on loosely coupled independent functions running on collaborating LocalDomains, business partners exchange data across systems. Each system independently handles its own data and, when required, draws data from the database and sends it to another system. A counterpart receiving function enables data to be included in the local database. A common format is decided for data transmission that leaves business partners fully independent as to managing data internally.

The two models are not used rigidly. A trans-European network may use varied combinations of the two models. An 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 (or even to a wider user community on the Internet.)

4.3.2 Content interoperability
Both models refer to XML as the standard foundation for exchanging content. Because information is itemised and encapsulated inside custom-defined tags that contain semantic information about data, XML provides the means for defining information structures as a set of granular, manageable components. These components can be created, expanded, searched, changed, managed and linked to one another in real time by means of all XML-enabled software.

Interoperability standards recommended by IDA use XML and XML schemas as the underlying protocol for data exchange and process management.

The project MoReq (Model Requirements for the Management of Electronic Documents)\(^4\) is to be referred to for functional requirements for electronic records management.

The MIReG project ('Managing Information Resources for e-Government')\(^5\) aims to extend the Dublin Core metadata set to meet the additional and specific requirements of public administrations. MIReG is intended to define both the proposed metadata set and a framework for its effective use.

4.3.3 Technologies
The described services are implemented using the following technologies.

**SOAP and Web services**
SOAP (Simple Object Access Protocol) is a W3C standard defining an XML-based architecture 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.

Building on SOAP, an innovative model called Web Services is gaining increasing success in the e-business world. Web Services enable a single business process to be seamlessly carried out by applications running on multiple web services.

Although the services could support the application-to-application communication model by allowing systems to interoperate synchronously, they may however impose operation constraints on collaborating LocalDomains.

\(^4\) http://europa.eu.int/ida/en/document/2303
Therefore the use of web services is only suitable for server-side processing within a simple transactional model. This approach enables a large degree of reusability. Because Web Services allow a process to be collaboratively run by independent systems, a given piece of functionality can be designed once to serve multiple projects. (An example taken from the e-commerce world: in a web shop, 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 application for follow-up).

**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.

**Java and J2EE**

Java is the software development standard recommended in these guidelines. J2EE is the related component development model. The combination of J2EE and XML provides a sound and sufficiently mature foundation to build server-side applications providing any of the above services.

It should be noted that Java is not mandatory for partner National agencies. EU agencies are invited to use Java, instead, for maximum component reusability.

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

- **Dynamic HTML Pages**
- **JSP Pages**
- **Enterprise Beans**
- **Database**
- **Client tier**
  - Client machine on a “user” LocalDomain
- **Web tier**
  - J2EE Server on a “common” LocalDomain
- **Business tier**
  - Enterprise information system tier
  - RDBMS or “legacy” systems on a “common” LocalDomain

The following diagram illustrates how J2EE is used to implement the application-to-application communication model:

- EbXML for asynchronous communication, or
- Web Service specification for synchronous communication
4.4 Data presentation and exchange

Within the context of the IDA community, the most common user interface will be a computer screen, generally with a web-based, graphical user interface. In this respect, general principles of ergonomics and user-friendliness should be taken into account. With respect to web-based applications, the Web Content Accessibility Guidelines have been adopted as a common standard. These guidelines take into account the special requirements for disabled persons.

The design of interfaces of mobile equipment such as PDAs or mobile telephones must take into account the emerging standards for WAP and i-Mode.

The basis for agreements regarding the content, file format, exchange and storage of the various types of data (short messages, documents, graphics (static and moving image), sound, video) is governed by standards that include SGML, HTML, XML, DSSSL, EMI, UML, WebDAV, TXT, PDF, GIF, TIFF, JPEG, MPEG, CGM, VMP, ZIP, and formats for SMS messages and i-Mode interfaces.

To ensure the exchange at the level of characters of text (in any file type), standardisation of the underlying character sets is arranged by the Unicode standard, which takes into account the multilingual requirement of the entire range of diacritical characters.

Access to information, documents and services, and the interoperability between systems necessary to deliver access, is facilitated by metadata. Most, if not all Member States and European institutions are developing metadata models to describe their information holdings. The development of a metadata model based on the Dublin Core metadata model and these national models will assist access to public sector information and the development of trans-border government e-services.

4.4.1 Services and tools

Simple web interactive service
This service is based on a transactional model using a standard light client (browser) and standard protocols (HTTP, XML). It approach should be used whenever possible on account of the universality of the client and its simplicity, enabling even large-scale deployments without client installation. 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.

Interface complexity is conveniently handled using W3C standards such as DOM and CSS. Whenever the required complexity of the interface requires supplementing the browser’s native interface, Java applets may be used on the client side.

Application to application messaging
This service uses an approach of loosely coupled independent functions running on collaborating LocalDomains. It is an EDI-type approach that involves using either standard XML schemas or locally defined business messages over an asynchronous, store-and-forward communication platform.

Portal technology
A portal solution is a set of tools that allows integration of disparate services and contents into a coherent whole that is made available to users via the web.

Portals primarily address communities and meet the requirements of independent organisations that wish to share contents or to give their audience a coherent service (e.g. government portals). An ideal portal solution should integrate standard Internet-based technologies referred to in these guidelines, offering a managed set of services to ease service customisation, content administration, user profiling, identity management, security, site administration.

Portal services provide a single gateway to disparate data sources, and as such they offer the following advantages:
deliver front-office services that are tailored to individual users, based on user profiling. Users are enabled to configure the information service to their own requirements in term of both content and presentation, and even to receive the same amount of information on multiple terminal types (PC, WAP, SMS, etc.);

concentrate related information coming from multiple sources, in such a way that the user refers to a one-stop entry point;

offer users a simple access mechanism instead of the technical complexity of accessing disparate data sources;

ensure data integrity across transactions and integration of front office and back office - to this end portal architectures are built upon transaction management platforms.

Relevant developments and examples of portal projects in the context of the IDA platform include:

open source toolkit for collaborating portals;

eLink is a middleware solution developed by IDA which provides a range of services for information exchange primarily between public sector authorities. It also caters for data exchange between citizens and the public sector, and enterprises and the public sector;

the portal of the EU Administration (public-services.eu) – this project addresses the need to establish a portal framework. The focus of the portal is the provision of online information and services in support of the freedom of movement of citizens and enterprises throughout Europe.

CIRCA
CIRCA (Communication and Information Resource Centre Administrator) is a web-based environment providing on-line-services that offers a common virtual space for workgroups and networks, enabling the effective and secure sharing of resources and documents.

The CIRCA service is available for users from Public Administrations. It is accessible via the Internet and also via TESTA (see below, network services). It is organised around interest groups, i.e. a private workspace for a group of people that need to collaborate in order to achieve common objectives and tasks. Although all groups have access to the same set of functionality, the environment is fully customisable for a given interest group and the information is restricted to the members of that specific group or various functions such as chairman, contributor, secretary, and member.

CIRCA offers the possibility to replicate such functions by providing for different access classes, thus customising users’ access rights to specific data elements, functionalities and operations in the I/G. A specific access class, the Leader, is granted extra privileges.

4.5 Security Services
An integral part of the security policy is the infrastructure security policy, defining security-enforcing mechanisms that are implemented by specialised software/hardware components. In a trans-European network context, security spans several layers: physical, operating system, network and application.

- **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 reinforce 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 ISO 17799 – Code of Practice for Information Security Management 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, ISO 17799 also provides guidance on related security issues, such as policies, security awareness, business continuity planning, etc.

### 4.5.1 Information System security implementation

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

- the Interconnection security implementation to be built at the EuroDomain or Internet level
- 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 3, IS security implementation](image-url)

It is important to state that security implementations must coexist, interoperate and be monitored within specific Security Service Level Agreements between the LocalDomain and the Interconnection 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 Interconnection Service Provider apply to external third parties.

### 4.5.2 Application security scope

Any application security policy for an application located inside a LocalDomain and using EuroDomain should consider the security level given by EuroDomain and define its own security ruling accordingly.

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.
<table>
<thead>
<tr>
<th>Security Layer</th>
<th>Protection needed</th>
<th>Where</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td>Yes</td>
<td>For application user access and for access to IP generic services.</td>
</tr>
<tr>
<td>Network Security</td>
<td>Yes</td>
<td>For monitoring and auditing network accesses.</td>
</tr>
<tr>
<td>Operating Systems Security</td>
<td>Yes</td>
<td>For application servers in LocalDomains.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Yes</td>
<td>For accessing application environment.</td>
</tr>
</tbody>
</table>

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

To establish a security policy, risk analysis should be performed inside each domain concerned. The risk analysis should comprise the following activities:

• definition of all resources under consideration (i.e. information and assets that are used to handle information, such as software, hardware, network devices, etc.);

• assessment of the sensitivity of these resources (based on the amount of damage that the organisation would suffer in case of a security breach affecting each resource);

• definition of potential threats to these resources and assessment of their degree of severity (based on some weighting criteria to evaluate the threat agent’s capability to cause damage, the agent’s motivation or the event’s likelihood);

• definition of the vulnerabilities of each of the resources that could be exploited by the threats, and evaluation of the degree of weakness of each vulnerability.

This assessment results in a risk matrix that allows an analyst to examine each resource for sensitivity against its weaknesses and the severity of the threat. Because sensitivity, weaknesses and severity are given evaluation marks, the analyst obtains numeric risk indicators for each of the resources under examination.

The last stage is to define countermeasures for each risk, using ISO 17799 standard controls. Choosing controls is the responsibility of the planners, based on a cost-benefit analysis (each countermeasure’s cost is evaluated against the damage it is designed to counter, expressed in economic terms).

Inside a LocalDomain, controls must be established within the constraints set out by the user community as a whole. The constraints impose a set of security controls on the LocalDomain planners who cover the common business (e.g. on information exchange or on access to common resources).

4.5.3 A PKI for trans-European projects

The IDA Public Key Infrastructure for Closed User Groups (IDA PKICUG) offers an effective, standards-based end-to-end security solution. The IDA PKICUG establishes a trust infrastructure at the pan-European level and can provide all the necessary services for the management of electronic certificates (creation, revocation, renewal) for members of IDA sectoral networks. IDA electronic certificates can also be used when no national Certification Authority (CA) exists, or when for any reason the users do not wish to use the services of the national CA. It should be complementary and interoperable with the infrastructures set up by the Member States, the European Institutions, and the European Commission, and able to harmonise the mutual recognition of certificates delivered by these infrastructures.

The services provided by the IDA PKICUG are:

• server authentication, i.e. a guarantee to the user that they are accessing the correct server, not to a false one (that kind of situation is called a "masquerade");

• client authentication, i.e. a guarantee that the server is able to authenticate the identity of the user, not someone masquerading as the user;

• confidentiality, i.e. encryption of exchanged data with a key that only the user and the server know;

• electronic signature, i.e. on electronic documents and on e-mails;
• non-repudiation, i.e. services that are designed to prevent a sender from denying to have sent information or a recipient from denying to have received information.

The security needs of the IDA-CUG communities will be met by using:

• personalised procedures, adapted to the organisation of each user community, and to their needs;

• a common root certificate, completed by sub-root certificates, that will create and sign only the certificates of an identified group of users, after the approval of the competent Registration Authority; and

• the secure infrastructure and the experience of a trusted CA for managing certificates.

IDA PKICUG’s certificates follow the X.509 v3 standard, and have no critical extensions. The services are provided by using products that comply with the S/MIME and SSL protocols, used in conjunction with TCP to establish secure point-to-point dialogues. Most common web servers and clients (browsers) use SSL, and S/MIME for secure electronic mail, to introduce security into web connections through the use of asymmetric cryptography techniques.

To request and receive a certificate, all that is required is a computer with a standard web browser, access to either TESTA or the Internet, and access to e-mail.

The IDA PKICUG works with most common browsers. However, the most recent versions of browsers, preferably the 128 bit enabled versions, are recommended as they are more user friendly concerning security management.
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:

<table>
<thead>
<tr>
<th>Type of process and type of content</th>
<th>This information helps you to identify a particular process within the business requirement category.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanism description and security requirement class</td>
<td>This information provides an outline of the solution that matches the selected requirement.</td>
</tr>
<tr>
<td>Services</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• a client part – services that run on the client workstation;</td>
</tr>
<tr>
<td></td>
<td>• a user LocalDomain – services that run on the network of the partner organisations;</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Security</td>
<td>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.</td>
</tr>
</tbody>
</table>

- Consult the diagram in paragraph 5.3 for a graphical representation of the various solutions, within the context of the entire architecture.

- Consult the service descriptions in the Annex to these Guidelines 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

<table>
<thead>
<tr>
<th>General requirement context and outline</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes in which relevant data is gathered from distributed sources (i.e. multiple LocalDomains) potentially across the EU into a common EU database (hosted on a LocalDomain belonging to a coordinating organisation e.g. the Commission, Agencies, etc.). This model is suitable when a central organisation is responsible for, or is simply willing to provide, support or coordination services.</td>
<td>Data collection, see Category 1</td>
</tr>
<tr>
<td>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.</td>
<td>Data exchange, see Category 2</td>
</tr>
<tr>
<td>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).</td>
<td>Data dissemination, Category 3</td>
</tr>
<tr>
<td>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.</td>
<td>Data sharing, see Category 4</td>
</tr>
<tr>
<td>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.</td>
<td>Alerts, see Category 5</td>
</tr>
<tr>
<td>Service processes, supplementary to all others.</td>
<td>Services, see Category 6</td>
</tr>
</tbody>
</table>

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 categories are 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.


The security categories used in the roadmaps only cover information that the Decision refers to as “non-classified”, 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 classified as “EU RESTRICTED”, EU CONFIDENTIAL, EU SECRET and EU TOP-SECRET is outside the scope of these guidelines and is to be dealt with on a case-by-case basis according to the security decisions 2001/264/EC and 2001/844/EC. Please refer to the Official Journal of the European Communities for the text of these decisions, [http://eur-op.eu.int/general/en/oj_en.htm](http://eur-op.eu.int/general/en/oj_en.htm).

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:

<table>
<thead>
<tr>
<th>Generic service</th>
<th>Usage</th>
<th>Reference to requirement category</th>
</tr>
</thead>
</table>
| 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 electronic signature or server or client authentication is 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:

<table>
<thead>
<tr>
<th>Area</th>
<th>Tools and techniques</th>
<th>Description</th>
<th>Data exchange</th>
<th>Data collection</th>
<th>Data dissemin.</th>
<th>Data sharing</th>
<th>Alert system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application services</td>
<td>CIRCA</td>
<td>Web-based environment offering a common virtual space for work-groups and networks, enabling the effective and secure sharing of resources and documents.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IDA-QA</td>
<td>Quality programme aimed at facilitating the achievement of business needs in trans-European projects by defining QA guidelines and generic self-assessment tools.</td>
<td>X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IDA-MT</td>
<td>&quot;Machine Translation for IDA networks&quot;, covers a series of projects aimed at providing effective and user-friendly access to the European Commission's machine translation (MT) system for the interchange of multilingual data between European public administrations.</td>
<td>X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content interoperability</td>
<td>MoReq</td>
<td>Comprehensive specification of functional requirements for the management of electronic records.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MiReq</td>
<td>Production of a metadata framework for government information in pan-European applications, with associated vocabulary control, ontologies and topic maps, and best practice guidelines.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Front Office</td>
<td>Global Search*</td>
<td>A &quot;one stop&quot; service that provides search facilities for relevant EU information regardless of its physical location. Special attention is given to the multilingual aspects of EU information.</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Back Office</td>
<td>STATEL</td>
<td>An API library and a command interface offering a transparent service for bi-directional file transfer.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eLink*</td>
<td>eLink is a middleware solution developed by IDA which provides a range of services for information exchange primarily between public sector authorities. It also caters for data exchange between citizens and the public sector, and enterprises and the public sector.</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Use of Open Source software</td>
<td>Information about the use of open source software in public administrations</td>
<td>X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Under development

Use of these tools, when appropriate to the business requirements at hand, is strongly encouraged. As new tools are constantly being developed and others are being evaluated, please consult the following URL for actual information: [http://europa.eu.int/idabc](http://europa.eu.int/idabc).

In addition to the use of generic services and common tools, the re-use of software and the use of open source software is recommended. For more information please refer to section 3.7 of the Annexes, the Open Source Software section of the IDA website[^6], and the IDA feasibility study ‘Pooling Open Source Software’[^7].

**Disclaimer**
Please note that the solutions illustrated in the following tables are based on best practice considerations. The information on security only covers with information that the Council Decision refers to as “EU non-classified”. 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.

---

### Requirement category 1, Data collection

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client</td>
<td>User Local Domain</td>
<td>Common Local Domain</td>
</tr>
<tr>
<td>1.1</td>
<td>Transfer of data held by the sender in electronic format</td>
<td>Business documents held by the sender either revisable (RTF) or non-revisable (PDF or TIFF) to be centrally collected</td>
<td>A file is uploaded to a centralised repository via a webservice (Web post)</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>Webserver Document management system or simple file system</td>
</tr>
<tr>
<td>1.2</td>
<td></td>
<td></td>
<td></td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>1.3</td>
<td></td>
<td>Sending as an attachment to e-mail files for storage on a centralised repository</td>
<td></td>
<td>Normal</td>
<td>e-mail client</td>
<td>e-mail account</td>
</tr>
<tr>
<td>1.4</td>
<td></td>
<td>Structured data between processes</td>
<td>Application to application (data is processed locally and converted to an agreed business message)</td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>1.5</td>
<td></td>
<td>Structured data to be fed to a Common LocalDomain</td>
<td>A web-based forms-type transactional application is used to collect data</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>Webserver Application server Servlet, EJB, JSP, JDBC RDBMS</td>
</tr>
<tr>
<td>1.6</td>
<td></td>
<td>Structured data</td>
<td>A web-based forms-type transactional application is used to collect data</td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>1.7</td>
<td></td>
<td>Structured data</td>
<td>A web-based forms-type transactional application is used to collect data</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>Webserver Application server Servlet, EJB, JSP, JDBC RDBMS</td>
</tr>
<tr>
<td>1.8</td>
<td></td>
<td>Structured data</td>
<td>A web-based forms-type transactional application is used to collect data</td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
</tbody>
</table>

*Architecture Guidelines V 7.1*
### 5.2.5 Requirement category 2, Data exchange

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Client</td>
<td>User Local Domain</td>
<td>Common Local Domain</td>
</tr>
<tr>
<td>2.1</td>
<td>Initiated by the sender</td>
<td>Data on business documents held by the sender either revisable (RTF) or non-revisable (PDF or TIFF) to be sent to peer LocalDomain</td>
<td>Direct e-mail between LocalDomains</td>
<td>Normal</td>
<td>e-mail client</td>
<td>e-mail account Optional: Notary service (ref)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Option: notary service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td></td>
<td></td>
<td></td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>2.3</td>
<td></td>
<td>Direct Web post to counterpart LocalDomain</td>
<td>Normal</td>
<td>Browser</td>
<td>on the recipient’s LocalDomain: - Website - Document management system or simple file system</td>
<td>Optional: Notary service (ref)</td>
</tr>
<tr>
<td>2.4</td>
<td></td>
<td></td>
<td></td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>2.5</td>
<td></td>
<td>Web post to a centralised message routing service</td>
<td>Normal</td>
<td>Browser</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td></td>
<td>Structured data to be fed to a central notification management system</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>--</td>
<td>Webserver Doc. management system or simple file system Application for message management and routing, delivering as in 2.9 or 2.11</td>
</tr>
<tr>
<td>2.7</td>
<td></td>
<td>A web form-based transactional application is used to collect notification data</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>--</td>
<td>Webserver, Application server, Servlet, EJB, JSP, JDBC, RDBMS Application for message management and routing, delivering as in 2.9 or 3.3</td>
</tr>
<tr>
<td>2.8</td>
<td>Structured data between processes</td>
<td>Liebel, (data processed locally and converted to agreed business message)</td>
<td>Normal</td>
<td>Dependent on technology used locally</td>
<td>EbXML, SOAP implemented on platform of partner org.</td>
<td>Optional: Notary service (ref)</td>
</tr>
<tr>
<td>2.9</td>
<td>Structured data between processes</td>
<td></td>
<td>Normal</td>
<td>Dependent on technology used locally</td>
<td>EbXML, SOAP implemented on platform of partner org.</td>
<td>Optional: Notary service (ref)</td>
</tr>
<tr>
<td>2.10</td>
<td>Initiated by the recipient</td>
<td>Generic document</td>
<td>Download data from website / post box</td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
<tr>
<td>2.11</td>
<td></td>
<td></td>
<td></td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
</tr>
</tbody>
</table>

**Architecture Guidelines V 7.1**
### 5.2.6 Requirement category 3, Data dissemination

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

Architecture Guidelines V 7.1
## 5.2.7 Requirement category 4, Data sharing

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access to shared areas for co-authoring</td>
<td>Structured XML documents for collaborative editing, plus communication frame for online communication</td>
<td>Connect to web-based collaborative environment &amp; retrieve: - document structure - text objects - multimedia Capability to upload and attach locally-edited components to XML document</td>
<td>High</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>User-ID &amp; Password on Common Local Domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authentication, Access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Consistency, integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Non-repudiation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>Search-based, information that may be present or not</td>
<td>Structured XML documents for collaborative editing</td>
<td>Search engines &amp; Indexing engines</td>
<td>High</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>Collaborative environment to send XML-based query form to user and to return a result list on: - documents; - revisions; - related documents - etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authentication, Access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Consistency, integrity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Non-repudiation</td>
</tr>
</tbody>
</table>
### 5.2.8 Requirement category 5, Alerts

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Confidentiality</td>
<td>Consistency, integrity</td>
<td>Authencticy, Access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Client</td>
<td>User Local Domain</td>
<td>Common Local Domain</td>
<td>SMIME</td>
</tr>
<tr>
<td>5.1</td>
<td>Push-type, urgency moderate</td>
<td>e-mail-based alert message</td>
<td>E-mail an agreed structured message, digitally signed by sender</td>
<td>High</td>
<td>e-mail client</td>
<td>e-mail account</td>
</tr>
<tr>
<td>5.2</td>
<td>Push-type, urgency high</td>
<td>Interrupt-based alert message</td>
<td>Agent placed on desktop via JVM</td>
<td>High</td>
<td>JVM</td>
<td>User-ID &amp; Password on Common Local Domain</td>
</tr>
<tr>
<td>5.2</td>
<td>Pull-type, urgency moderate</td>
<td>Document-based information</td>
<td>Internet publishing – Centralised Portal with high customisation (customised “what’s new” sections to be assembled “on-the-fly” presented individually to users upon logon)</td>
<td>Normal</td>
<td>Browser (XML, HTML, XSLT, DOM, Applets)</td>
<td>Web portal with user profiling – Functionality includes capability for administrators and users to tailor services upon user profiles</td>
</tr>
<tr>
<td>5.4</td>
<td></td>
<td></td>
<td>High</td>
<td>same as above</td>
<td>same as above</td>
<td>same as above</td>
</tr>
</tbody>
</table>
## 5.2.9 Requirement category 6, Service process

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Type of process</th>
<th>Type of content</th>
<th>Mechanism description</th>
<th>Security Req. Class</th>
<th>Services</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Client</td>
<td>User Local Domain</td>
<td>Common Local Domain</td>
<td>Authentication, Access control</td>
</tr>
<tr>
<td>6.1</td>
<td>Acknowledgement</td>
<td>Notification message, returned by the recipient of a data exchange to the sender</td>
<td>E-mail an agreed structured message, digitally signed by sender</td>
<td>High</td>
<td>e-mail client</td>
<td>e-mail account</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>Notary</td>
<td>Notification message, to be sent by a user who carries out a transaction to a central notary system</td>
<td>E-mail an agreed structured message, digitally signed by sender</td>
<td>High</td>
<td>e-mail client</td>
<td>e-mail account</td>
</tr>
</tbody>
</table>

*Architecture Guidelines V 7.1*
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 that serves “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 of a given service to counterpart organisations in the Member States.
  - LocalDomain “A” operates as follows:
    - The link A-B enables document exchanges with counterpart LocalDomain “B” using ebXML (or a subset thereof) and SOAP. (See requirement type “data exchange” in the roadmap.)
    - The link A-C 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.)
    - The link A-D 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.)
    - The link A-E is used by LocalDomain “A” to access 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. This tool provides 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.
Figure 4, Interoperability between LocalDomains