Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Technical description of target eGov infrastructure for delivering PEGS

Specific contract n°5 based on ENTR/02/20-EGOVERNMENT (Contract IDA.20040539)

Architecture for delivering pan-European e-Government services

Version 1.0

TABLE OF CONTENTS

1 MANAGEMENT SUMMARY

Pan-European e-Government Services (PEGSs) will enable citizens and businesses from all Member States to access e-Government services in all Member States. In future these services will eliminate or reduce the current limitations on the free flow of people, goods, capital and services across all Member States of the European Union.

The road towards this goal has to overcome a number of hurdles of different complexity. An architecture has been developed that addresses these complexities and defines a range of solutions to overcome these hurdles. The extreme ends of this solution range can be characterised as follows:

1. Develop Communal Guidelines that define for each PEGS exactly how Member States would have to behave in order to achieve totally equal treatment of all citizens and businesses within the European Union. All efforts to achieve the full and unrestricted implementation of such Communal Guidelines, would be completely the responsibility of the Member State Governments.
2. Develop a kind of gateway that exactly defines how each PEGS could inter-work with other PEGSs within European Union without any change in its national context. All efforts to implement this gateway would be the sole responsibility of the European Commission.

Between these extremes a number of intermediate solutions have been defined. The architecture presented in this paper allows to mix and match all solutions according to different needs for different PEGSs, different political context to achieve Communal Guidelines, different inherent security requirements for different types of civil or business services or for administrative co-operation, different speeds of implementation for different and in future more Member States, and different maturity of ICT technology available in different Member States to implement these solutions.

The spectrum of solutions can be well described in terms of the European Interoperability Framework, developed by the IDA program in parallel to this architecture study. Existing initiatives by the European Commission like the (s-)Testa backbone network and the e-Link pilot fit well within this architecture, but as such only constitute building blocks, and are not solutions on its own.

It is anticipated that portal technology will unlock the potential of this European Inter-working Architecture to its users: citizens, as well as business representatives and civil servants, working for Member State Administrations. The real benefit however, comes from the application of the various integration scenarios of back offices of the participating Member State Administrations.

In order to implement any of the solutions outlined by this architecture a more detailed description and analysis of a representative number of specific PEGSs is a prerequisite. This document doesn’t describe any PEGS, but defines the services required that constitute the infrastructure for IDABC that would enable the full range of solutions, enabled by the architecture.

2 INTRODUCTION

2.1 OBJECTIVES

The objective of this project is to define the high level architecture needed to deliver pan-European e-Government services (PEGS).

To this end, three major deliverables are prepared:

- a document giving the functional requirements for this architecture (Requirement synthesis document, ref. (1));
- a document on technology and market trends relevant for the delivery of PEGS (Trends document, ref. (2));
- a document describing the technical infrastructure needed for the delivery of PEGS (Architecture document).

This is the Architecture document which describes the technical infrastructure for delivering PEGS.

2.2 SCOPE

The project deals with the support infrastructure that needs to be put in place to achieve interoperability at pan-European level.

Many Member States have already implemented national interoperability frameworks and middleware that allows the integration of different administrations at national, regional and municipal level.

The PEGS Infrastructure project is defining the additional components that are needed to support e-Government services at the pan-European level.

Since it allows to link up national middlewares, it can be seen as a “middleware of middlewares”.

The project is dealing with the architectural aspects of the infrastructure. It does not cover implementation.

However, where possible, we will point to implementation issues.

2.3 INFORMATION RESOURCES

(1) PEGS – Requirements Synthesis Document; Version 3.1; November 2004

(2) PEGS – Technology and Market Trends ; Version 1.1 ; October 2004

(3) EUROPEAN INTEROPERABILITY FRAMEWORK FOR PAN-EUROPEAN EGOVERNMENT SERVICES, IDA working document - Version 4.2 – January 2004

(4) Architecture Guidelines For Trans-European Telematics Networks for Administrations; Version 7.0

(5) IDA eLink specification; October 2003

2.4 APPROACH

2.4.1 General approach

The approach that was used is based on the Integrated Architecture Framework (IAF). Therefore we first start with a discussion of this framework.

The next figure shows the general IAF framework.

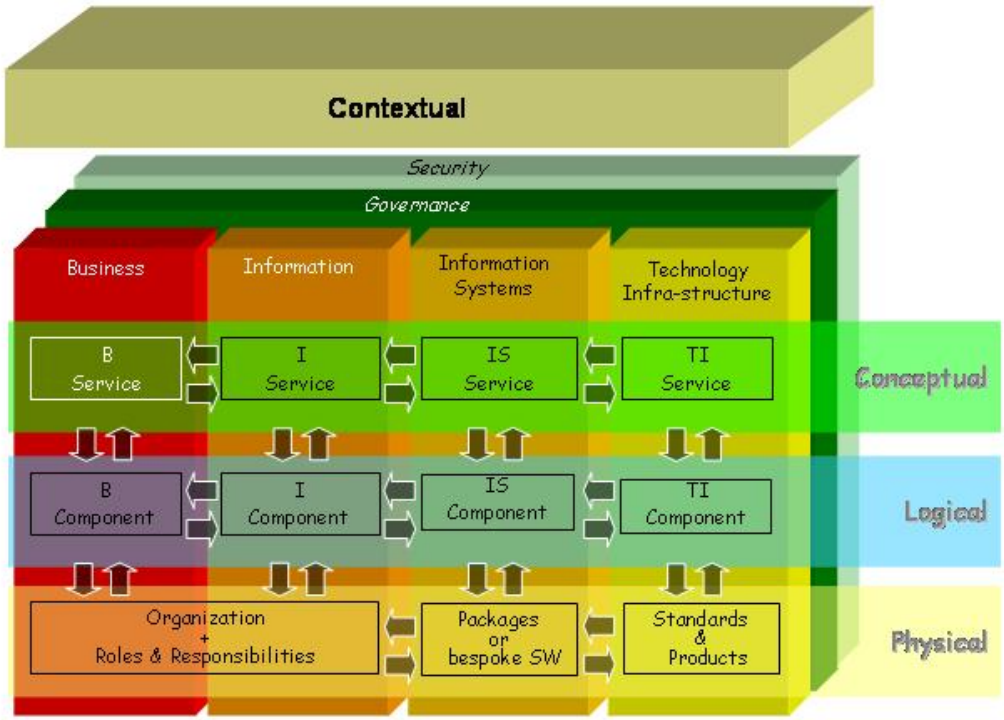

Figure 1 IAF Framework

The IAF addresses four architecture Aspect Areas: Business, Information, Information Systems and Technology Infrastructure. There are strong interdependencies between each of the aspect areas. For example, the business structure determines the information structure that, in turn, prescribes the structure for IS, which determines the technology infrastructure structure.

Ideally all aspect areas have to be incorporated in the architecture design.

There are two specialised Aspect Areas in IAF: governance and security. Both emphasize quality aspects of the architecture. They need to address all other aspect areas by nature and thus are positioned in another dimension.

Furthermore IAF recognises four levels of abstraction: contextual, conceptual, logical and physical. The first, contextual, is for answering the "why" question and to provide context information and key principles that supports the value proposition for the architecture to be developed.

The conceptual level addresses the "what" aspect of architecture design. It defines the services that are required and what is required from each service.

The logical level derives "how" the customer needs can be realised, showing how components interrelate and where components 'implement' services.

The last, physical, level addresses the "with what" aspects of architecture design and defines the standards, products (catalogues), guidelines, etc. for further development and implementation.

2.4.2 Specific approach used in the definition of the PEGS architecture

In an attempt to describe the context we first defined the principles which will govern the new architecture for the delivery of PEGS. Principles are guiding statements about fundamental beliefs, truths, rules and qualities that guide objectives and the decision making process. Architecture is linked to business needs through these principles. The principles were deduced from documents and refined during a debate with delegates of the Member States on October 19th, 2004. These principles are defined in chapter 3.

The architecture is intended to provide services to the business. To determine these supporting services normally an analysis of business processes is performed. In this case, the business processes (PEGS) are not known in advance. The architecture should be flexible and scalable to accommodate a wide variety of pan-European e-Government services.

To replace the business process analysis, we have considered a representative set of e-Government services that are eligible for cross-border extensions. For these PEGS we have defined the infrastructure services[1] that are needed to support the pan-European aspect. These services have been documented in the Requirements synthesis document.

We have defined four interoperability layers based on the European Interoperability Framework. We have mapped the services defined in the Requirements synthesis document to these layers, and to the Security and Governance aspect areas.

In this way we have defined a Conceptual Architecture, defining "what" has to be performed.

In the Logical Architecture we have defined alternative approaches for inter-working between Member State Administrations (MSAs). Also, detailed descriptions of the interoperability architecture are given.

[1]] "Services" defined here in the context of Service Oriented Architectures.

Finally, the physical architecture determines the applicable technologies and standards such as determined in the Trends document.

3 CONTEXT

3.1 PRINCIPLES IN GENERAL

Based on commonly available information, validated during a meeting on October 19th, 2004 with experts from several Member States, a set of principles has been determined that generally drive all architectural decisions and choices.

The principles listed are not ordered in any way and may in certain cases have conflicting impacts on alternatives.

The principles have been formulated on the appropriate abstraction level as to help define the business requirements of the PEGS infrastructure. The PEGS infrastructure is designed to support PEGSs. The decision to implement a specific PEGS, and therefore the instantiation of certain derived business requirements is outside the scope of this document. The requirements derived from these principles therefore are only completely valid, if the assumption that the identified types of PEGSs will be implemented is true.

3.2 MAJOR PRINCIPLES

3.2.1 Four freedoms

Pan-European e-Government services shall contribute to and support the principles of free flow of goods, persons, capital, and services within the European community

Rationale

This is the fundamental principle underlying the existence of EU

Consequences

The architecture to support delivery of pan-European e-Government services may not pose additional barriers to the realisation of the four freedoms.

3.2.2 Subsidiarity

Governance and operational autonomy shall be implemented at the most decentralised level that is appropriate for the service at hand

Rationale

Based on the general subsidiarity principle that states that the Union does not take action (except in the areas which fall within its exclusive competence) unless it is more effective than action taken at national, regional or local level

Consequences

The architecture explicitly recognises differences in implementation of (e-)government services, and supports inter-working with the least possible level of standardisation requirements across administrations in different member states. Communal guidelines will only be necessary when transparent inter-working of services can not be achieved.

3.2.3 Transparancy

Pan-European e-Government services shall be provided in such a way that any complexities arising from the involvement of administrations from multiple Member States, is hidden to the citizens and businesses using the services

Rationale

This is a direct consequence of the Four Freedoms principle: citizens and businesses should experience no barriers in that respect.

Consequences

Each Member State Administration (MSA) will shield any service implementation differences with administrations in other Member States

3.2.4 One stop shopping

Public authorities across Europe shall inter-work and co-operate in a way to minimise the effort of citizens and businesses of supplying information already supplied to other public authorities for the same purpose

Rationale

Information submitted to any government administration on behalf of the performance of an (e-)government services, shall not have to be resubmitted to the same or a different administration for the same purpose.

Consequences

Each administration will accept data in formats acceptable in any Member State to the corresponding administration; data conversions that may be necessary to fulfil services in different or multiple Member States will be taken care of by appropriate back-office processing

3.2.5 Trust

Pan-European e-Government services shall strictly apply all legal protection of citizens and businesses, including confidentiality, privacy, openness of public information, integrity and non-repudiation

Rationale

Citizens and businesses must have the guarantee that their fundamental rights are preserved. They must be assured that all interactions with government are properly secured.

Consequences

PEGS shall be sufficiently protected against embarrassment and will not abuse the position of the government against citizens and businesses. PEGS shall not undermine public auditability of the governmental administrations. Information provided to an administration cannot be reused without permission for any other purpose.
PEGS shall preferably reap the benefits of Open Source Software. Open Source Software (OSS) by definition allows anyone to validate that the software actually does, what it claims and nothing else.

3.2.6 Multilingualism

Pan-European e-Government services will be available in any official language of the community without restriction

Rationale

This is a direct consequence of the basic principles of language equality and of the four freedoms.

Consequences

All administrations shall put mechanisms in place to be able to translate between eventually any pair of official EC languages. It is the citizen or business that ultimately decides in which official language (s)he communicates with the administration. It is not mandatory that all administrations will provide all services in all official languages; a minimum of two languages and the possibility to add more will be sufficient in many cases.

.

3.2.7 Multiple velocity

Member States or individual administrations within Member States have the freedom to commit to an individual timescale for implementing pan-European e-Government services at a community wide scale

Rationale

Depending on technical complexity and implementation effort it is acceptable that some Member States implement any PEGS earlier than others

Consequences

During an interim period some PEGS will only be implemented in a subset of Member States. Due to this fact some of the other principles will initially not be fulfilled across some pairs of Member States. Administrations do not have an opt-out for community wide PEGS implementation, and must commit to a time scale; the architecture however will explicitly support multiple timescales for multiple administrations

3.2.8 Performance

Pan-European e-Government services shall have predictable performance in any circumstances, including operation across Member States

Rationale

Each government service by nature will evoke certain elapsed time and quality expectations. PEGS will meet elapsed time and quality expectations that generally are very similar to the corresponding services within the Member States

Consequences

Inter-working mechanisms between services across the PEGS infrastructure shall include service level agreements between pairs of administrations across Member States. Service levels stated in these inter-working mechanisms must be derived from corresponding service levels for national services within Member States

3.2.9 Stability

Pan-European e-Government services shall be available around the clock at sufficient capacity regardless of implicit technical complexity

Rationale

Each government service will take appropriate measures so that it can be fulfilled in accordance with reasonable expectations of citizens or business

Consequences

Administrations may have to implement supplementary services, whenever existing national service levels are significantly below expected service levels in other Member States. In some cases these supplementary services can be provided by the interworking gateway. Service maintenance procedures may have to be adapted to support the continuous availability requirements

3.2.10 Consistency

Fulfilment of pan-European e-Government services must be consistent, regardless of the access channels used in different Member States

Rationale

A governmental transaction initiated through a channel in one Member State is part of the context for that citizen/business in any Member State. It should be avoided that citizens or business can claim benefits from different Member States simultaneously that are supposed to be mutually exclusive

Consequences

Administrations will implement or extend publish/subscribe mechanisms to various databases in order to include relevant context information for citizens/businesses across Member States. By publishing any relevant transactions between citizens or business and governmental organisations, any MSA is capable of deriving correct decision from all relevant information

3.2.11 Perennity

Records and archives kept by pan-European e-Government services shall withstand decay of electronic media and obsolescence of access equipment

Rationale

Authorities must take due precautions to guarantee integrity of authentic sources of information with respect to media deterioration and/or access equipment compatibility. E-government services must be independent of technological evolution, industrial innovation, copyrights, patents etc.

Consequences

PEGS shall implement open specifications[2] in order to avoid a situation that the technology evolution creates variances in equipment across Member States that impede unrestricted inter-operability. New “standards” must be backwards compatible.

[2]]For a definition of Open Specifications refer to the European Interoperability Framework, ref. (3)

4 CONCEPTUAL ARCHITECTURE

4.1 REQUIREMENTS ANALYSIS AND SCOPE

4.1.1 The European Interoperability Framework

The requirements analysis is based on the information collected in the Requirements Synthesis document (ref. (1)). Based on this document and the European Inter-operability Framework (EIF), ref.(3), we have classified Member State Administrations (MSAs) wishing to create PEGSs or wishing to inter-operate with existing PEGSs into four cases:

1. MSAs that run incompatible business processes and have a need to inter-operate. These MSAs have two choices to enable PEGSs:
    - Inter-work by means of a procedural adaptation provided by some kind of "procedural gateway". The business services to be implemented in this procedural gateway are described in section 4.2.
    - Provide procedural adaptation themselves. This may require some change in national legislation, and prior to that a European Communal Guideline that defines common terms of reference for the business processes executed by the PEGS. The solution may or may not be similar to the solution described in this document in Chapter 5. With this self provided adaptation in place these MSAs classify for the 2nd case.
2. MSAs that run compatible business processes but still do not have common semantics, i.e. they have similar business objects but do not share a common taxonomy for describing their business objects. They also may classify their business objects differently. Also organisations that have created business process compatibility by means of a self owned adaptation i.e. simulate to have similar business objects. These MSAs have two choices to enable PEGSs:
    - Inter-work by means of a semantic transposition provided by some sort of "semantic gateway". The information services to be implemented in this semantic gateway are described in section 4.3
    - Provide the semantic harmonisation themselves. This harmonisation often involves a change in the public awareness of certain business objects. Typically such a change is a long term process (many years) to become predominantly effective. In many cases efforts to harmonise certain parts of business object taxonomy have already been initiated in the past, and become increasingly effective. Many other harmonisation cases have not yet been addressed for various reasons. With harmonisation in place these MSAs classify for the 3rd case.
3. MSAs that run compatible business processes and have harmonised common semantics, may still not be able to exchange electronic data effectively, because

they may use different protocols, different languages, different character sets and different message formats. To enable inter-working between these types of MSAs, we have the following possibilities to inter-work:

- Inter-work by means of a technical conversion provided by a so-called "technical gateway". The information system services to be implemented in this technical gateway are described in section 4.4.
- Provide technical adaptation themselves. In many countries, in Member States as well as in other countries, initiatives have been taken to provide a national technical adaptation layer (middleware) that can fulfil this purpose. Alternatively, MSAs can provide technical adaptation themselves, individually or in co-operation with other MSAs. When technical adaptation is in place a MSA classifies for the 4th case.

4. MSAs that run compatible business processes, have harmonised semantics, and use common protocols, languages, character-sets, units and formats do not need any gateway, but require an interconnecting transport and network infrastructure.

   The services required by this interconnecting infrastructure are described in section 4.5.

In the following picture an overview is given of the four above mentioned classes of inter-working MSAs.

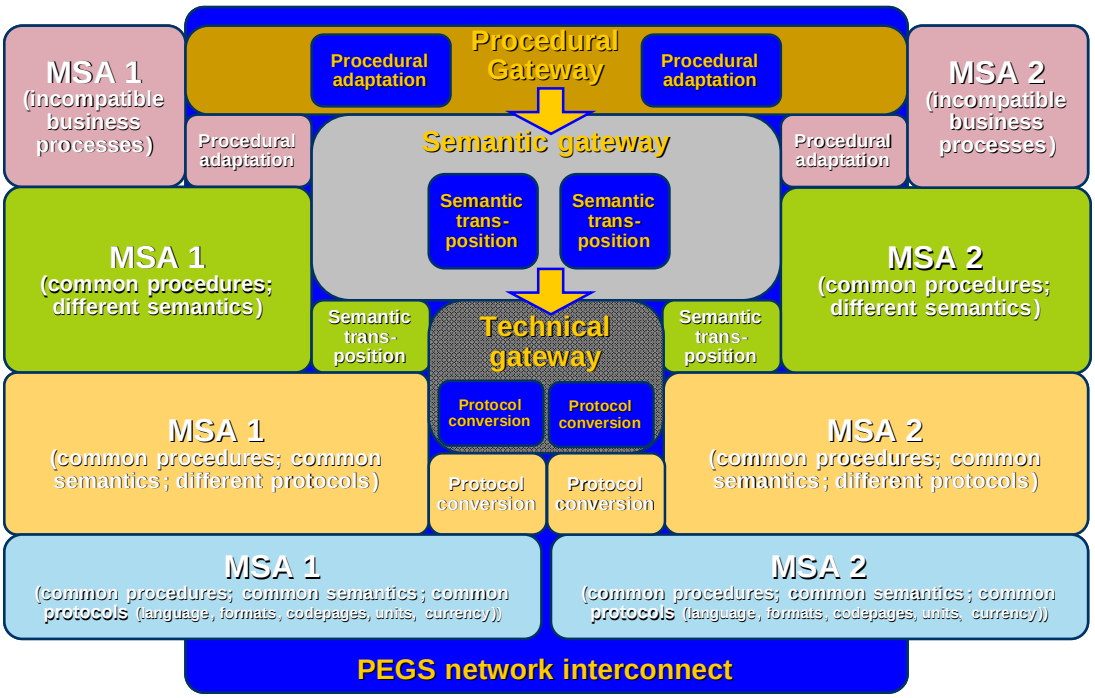

Figure 2 MSA Interworking

It is assumed that the concept of a procedural gateway can reuse the services defined for the semantic gateway. Likewise it is assumed that the concept of the semantic gateway can reuse the services of the technical gateway. It is also assumed that the technical gateway can use the services defined for the PEGS network interconnect.

Based on the above analysis, the scope of the PEGS infrastructure architecture includes (dark blue):

- The PEGS network interconnect;
- The technical gateway;
- The semantic gateway;
- The procedural gateway.

The implementation of PEGSs within the MSAs is considered out of scope.

The non-technical aspects from operating the various gateways defined in this section are also considered out of scope for the architecture.

An in-depth analysis of all services, needed for the cross-border operation of PEGSs can be found in the synthesis document, ref. (1).

4.1.2 Access to pan-European e-Government Services

PEGS will be accessed by three kinds of users, each with their specific requirements and expectations:

- Citizens accessing PEGSs in order to perform self-service e-Government services. Citizens want easy access in their own language to a wide variety of services. Data they enter should not by trackable to their identity, or should be exchanged within a secure context, that can reasonably be trusted by that citizen, and should apply a privacy policy strictly conforming to European guidelines.

  PEGS should be available in the language that is understood by the citizen, therefore they should be available in several official languages.

- Business representatives access PEGSs in order to perform self-service e-Government services on behalf of the organisations they represent. They want easy access to a wide variety of business oriented services in the local language or in the common business language of their organisation. In a majority of cases the business language will be English. Data they enter should be secure against competitors, and should not be mixed up in anyway with private data that may have been entered by them in their role as citizen.

- Civil servants access PEGSs in order to fulfil administrative tasks or to fulfil requests from citizens or businesses. Civil servants are likely to work with PEGSs on a daily basis, at least much more frequently than individual citizens are likely to do. Therefore extensive customisation support is necessary. To avoid any ambiguities or uncertainties, civil servants are urged to only have to use their own language. Security controls must be in place to guarantee a strict separation between access to PEGS as civil servant and personal access as citizen.

The next picture shows the three different roles and in addition three layers of information:

- Front-office information: available to anybody without identification
- Mid-office available to everybody with proper identification
- Back-office: only available to authorised persons on the basis of secure authentication.

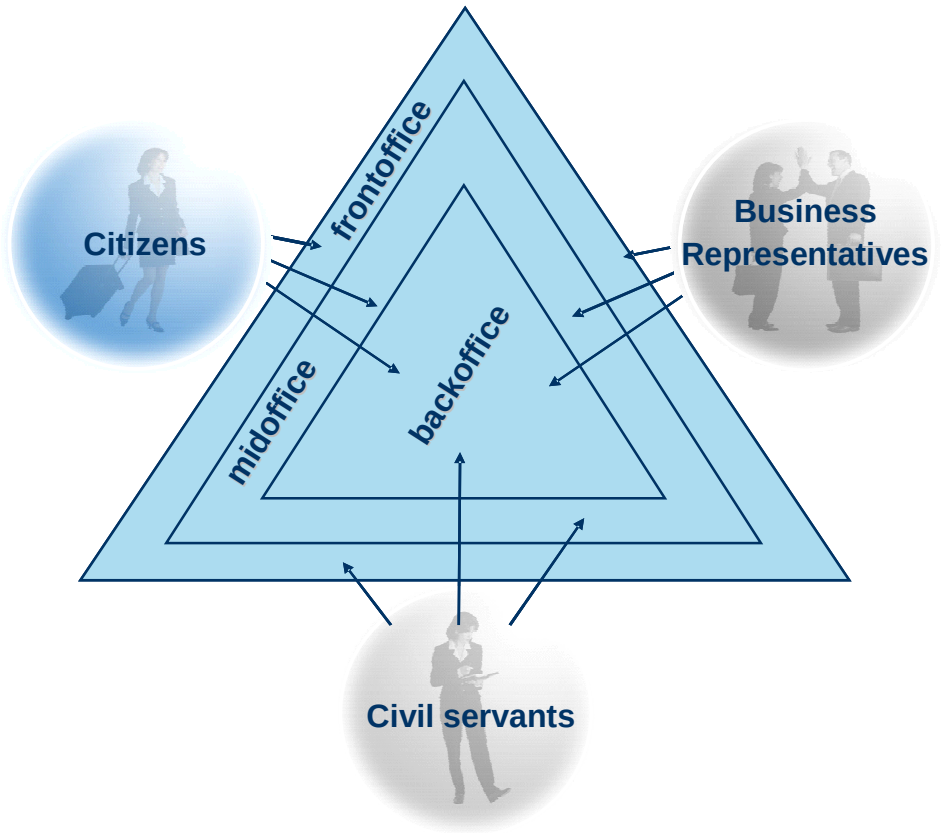

Figure 3 User roles

4.2 SERVICES IN THE PROCEDURAL LAYER

Pan-European e-Government Services (in this document further referred to as PEGS) are e-Government services that are made available across the EU to all EU citizens, businesses and Governmental organisations in other Member States. In most cases these service are derived from existing or planned e-Government services, or more generally from Government services.

The PEGS infrastructure needs to fulfil additional business services as part of the procedural gateway. The required services are derived from the synthesis document.

Business services	*Description*

Business services	*Description*
Case prioritisation	For some PEGSs rules have to be defined which unequivocally determine the priority that should be given to the handling of a specific case across Member States.
Inter-banking support	Existing national administrations may not be capable to handle international payment transactions on behalf of their operations. A national front-end banking account would disguise the international payment as a national payment. The service itself would just do the international transaction using standard Euro-banking services
Financial equalisation	Under the principle of the four freedoms, a citizen/business getting in contact with another Member State's administration should not pay more for an e-Government service than a citizen/business of that Member State. To achieve this, financial clearing services may be required in order to allocate differential charges elsewhere.
Workflow	Workflow allows combining different steps to be performed, possibly across borders. In the case of the PEGS infrastructure, a workflow service will be needed at the level of the procedural gateway where there is no simple mapping of processes. The workflow allows the mapping of different process steps, calculation of the expected response times and the monitoring of the results.
Replacement procedures	If mere transposition of needed documents is not possible, replacement procedures may have to be defined to get the required data.
Deadlock detection and resolution	To avoid and resolve situations where two PEGSs or MSAs are waiting for each other to complete a process step.

4.3 SERVICES IN THE SEMANTIC LAYER

The following information services have been identified as needed, either as part of a semantic gateway, or to support the business services defined in section 4.2.

Information services	*Description*
Combine information across borders[3]	It should be possible to combine information about citizens and businesses that is stored in multiple administrations, also when these administrations are located in different Member States, and potentially use different languages, different indexing methods and different business object taxonomy
Consult list of (transposed) document types	When performing a pan-European e-Government service, citizens, businesses and administrations may have to provide certain documents from one MS to the other. They should have an easy way to find out which documents are needed (possibly data needs of one MS need to be transposed in documents recognised by the other MS)
Management of metadata	The functionalities to create, maintain and consult the metadata on PEGS, exchanged data, data formats, conversions, etc.
Cross-border identification	When citizens/business are the subject of interaction between Member States, they need to be identified unequivocally.
Local identification of citizens	When a person stays in another Member State and gets in contact with a local administration, he/she should be identified in an analog way as is done for local residents.
Transpose data	In order to exchange certain data between MSAs a semantic transposition of this data needs to be performed.
Transposition of deeds	The transposition of legal documents in the legal framework of another Member State such that they reflect the legal dispositions that are in place in that Member State.
Coupling of call centres	When services are provided cross-border there may be a need to interlink call-centres of different Member States.
Legal process facilitation	Citizens or businesses should have the same rights in another MS as the citizens/businesses of that Member State. This implies that may need services to support them in legal matters[4].

[3]]This is a service that also is needed on lower levels. When considering implementations that start with the lower interoperability layers, (a subset of) this service may also be needed. This remark may also hold for other services.

[4]] Legal representation by lawyer is not meant here. Only the transposition of legal steps in one Member State into equivalent legal steps in another Member State is meant here. In a sense it is a service a lawyer should want to use to be equally effective across Member State borders.

Information services	*Description*
Yellow pages	PEGS with a need to exchange information with PEGS in other Member States will, except for common cases, not have the knowledge to determine in which case what type of conversion, adaptation or gateways are needed to inter-work. This ignorance will be aggravated when partial implementation, with changes over a time period (due to the multiple speed principle) inhibits straight inter-working across the appropriate type of gateway, when needed. A "semantic directory" service will solve this problem.

4.4 SERVICES IN THE TECHNICAL LAYER

The following are a minimal set of Information System services that must available to support a gateway on all of the levels described in the section 4.2 Business Services and section 4.3 Information Services, or to implement a technical gateway.

Information System Services	*Description*
Information available in multiple languages	Information made available by a Member State Administration to its citizens and businesses should also be provided in other official EU languages.
Message formats dictionary	In order to be able to send messages in a format that is acceptable for a specific MSA, the PEGS infrastructure must include a table of supported message formats.
Monitor outcome of a public service	Citizens and businesses must have the possibility to know what the outcome is of the execution of a public service. They must understand the outcome and be able to validate if all legal regulations have been correctly applied.
Find information on procedures to follow	Citizens, businesses and administrations should have an easy way to find what procedures apply for a specific e-Government service, which authorities to contact, etc.
Exchange of administrative records	Exchange of data between administrations of different Member States, including reformatting, language translation, conversion of measures and currency

Information System Services	*Description*
Submit declarations in own language and alphabet	When getting in contact with administrations, it should be possible for citizens and businesses to do this in their own language and alphabet.
Integration of GIS	It should be possible to produce geographic maps with consistent information of areas/regions across borders between Member States
Realtime / Neartime translation service	The translation of information between any pair of official EU languages in urgent exchanges by means of automated translation engines
Delayed / official translation service	The legally binding translation of information in non-urgent exchanges between any pair of official EU languages.
Perform unit conversions	For pan-European e-Government services between Member States using different units (such as currencies), a conversion between units, quantities and/or amounts must be performed.

4.5 SERVICES IN THE TRIVIAL LAYER

The following are a minimal set of Technical Infrastructure Services that must available to support any gateway on all of the levels described in the section 4.2 Business Services, section 4.3 Information Services, and section 4.4 Information system Services or to enable direct information transport between MSAs without a gateway. The core functionality of the Technical Infrastructure is to provide connectivity and associated services to all MSAs that wish to exchange information, now or in future.

Technical Infrastructure services	*Description*
Portals	A portal service gives the possibility to combine information from different MS Administrations and EC Institutions on the desktop.

Technical Infrastructure services	*Description*
Connectivity	Every MSA with a need to read, write, publish or subscribe to data that are also relevant for MSAs in other Member States must be connected to a common transport network, with sufficient bandwidth, either directly, by means specified by the operator of the common transport network, or indirectly by means of a national transport network that is connected to the common transport network
Addressing	Every MSA, each department within that MSA, and each civil servant working on behalf of that MSA should be addressable to all MSAs that provide PEGS, either by name, or by content
Bulk-data transfer	Any MSA should be capable to send data to other MSAs without an restriction on the volume of the data
Location of "authentic" physical documents	The location (Member State and Administration) of "authentic" physical documents must be determined across Europe. Also, when for some reason such documents have to move, the new location has to be determined.
White Pages	All persons[5], businesses and authorities with access rights to e-Government services for which authentication is required, must be registered in a communal (distributed) directory, or in a national, sub national or sectoral directory that is linked to by the communal directory
Redundancy	Each MSA that can be involved in PEGS with critical performance requirements, must be connected by at least two independent access channels to the transport infrastructure, which have no resources in common.

4.6 SECURITY SERVICES

The following are a set of Security Services that are needed to support the security and privacy requirements in the delivery of PEGS.

[5]] Citizens, business representatives , authorised civil servants

Security services	*Description*
Mutual identification and authentication of authorities involved	The (local) administrations that are involved in the fulfilment of specific pan-European e-Government services should be mutually identified and authenticated as the proper authorities for the specific exchange.
Role identification	Besides the cross-border identification of persons, their role should be asserted so as to make sure that they are authorised to execute the service and process the specified data. When there is no exact match in role definition between different Member States, a transposition needs to be performed. (This may be dependent on the specific service – e.g. it could be that exchange of medical information is in one Member State restricted to physicians, while in others it may also be performed by other medical staff.) (other roles: recognition of notary, …)
Access to remote data	Administrations must have access to remote data such as to preserve the consistency of public services.
Accreditation	The authorisation and approval granted to a MSA to process EU classified information in its operational environment. (COMMISSION DECISION of 29 November 2001 amending its internal Rules of Procedure to define the COMMISSION PROVISIONS ON SECURITY. A similar regulation exists for the Council, which is also binding on the Member States.) Less formally, this could be defined as the formal recognition that an information system operated by a MSA has the required security protection mechanisms for the protection of classified information in place.
Profile transfer	All profile data about users[6] of PEGSs that are marked for communal use will be transferred between implementations of PEGS across Member States, with automatic transposition of semantics
Monitor the use of personal data	Services that allow the citizen to monitor and control the use that is made of his/hers personal data.
Exchange of sensitive records	In some circumstances sensitive records (such as medical information) must be exchanged between authorised parties. Therefore information should be classified such that proper access rights can be transparently given across Member States

[6]] Citizens, representatives of businesses, call centre agents or civil servants

Security services	*Description*
Confidentiality	Services to guarantee the privacy of sensitive data (such as medical records). Confidential data should be properly encrypted when handled outside the seclusion of the intended audience.
Integrity	Services to guarantee that the content of a record – even when it has to be translated (language, units, currency, character set, segmentation) is not changed between sender and receiver
Non-repudiation	Service to guarantee that no ambiguity can exist whether a transaction took place or not and who authorised it
Authentication	Service to unambiguously get proof of the identity of a person (either citizen, business representative or civil servant), or a resource available to the PEGS infrastructure, or a MSA authorised to use the PEGS infrastructure
Identification	Service to allocate co-operative resources to the same requester

4.7 GOVERNANCE SERVICES

Following are a number of Governance Services that have to be provided. (We did not include general Governance services that deal with Program & Project Management, Planning and Control, Configuration & Change Management, etc. They are important, but not specific for the PEGS Infrastructure context)

Governance Services	*Description*
Monitor progress of a public service	Citizens and businesses must have the possibility to monitor the fulfilment of a public service, also when this service extends cross-borders.
Monitoring of SLA's	It should be possible to monitor the SLA's that are applicable for a given service.[7]
Manage SLA's	Services to add and maintain SLA's for specific PEGS.
Error reporting	Adequate reporting on problems with the normal execution of a PEGS.
Transaction management	Services to assure the integrity of data exchanges and related work (e.g. database updates) across borders that have to be treated as a unit of work.
Monitoring and measurement	Services to measure and monitor different components and characteristics of the PEGS Infrastructure; such as volumes, performance, availability…
Tracking and tracing	Services to trace messages within the PEGS Infrastructure. These services are needed for problem support and solving.

4.8 SERVICE CLASSIFICATION

The services described above can also be classified by the way they are accessed. This description is relevant because existing e-Government services will have to be changed or expanded to become PEGSs.

4.8.1 National Services

The working of National Services is visualised in the following picture:

[7] This is a service which should be available for citizens, businesses and civil servants so they know when results may be expected. It should also be available to applications to monitor automatically the execution of certain services.

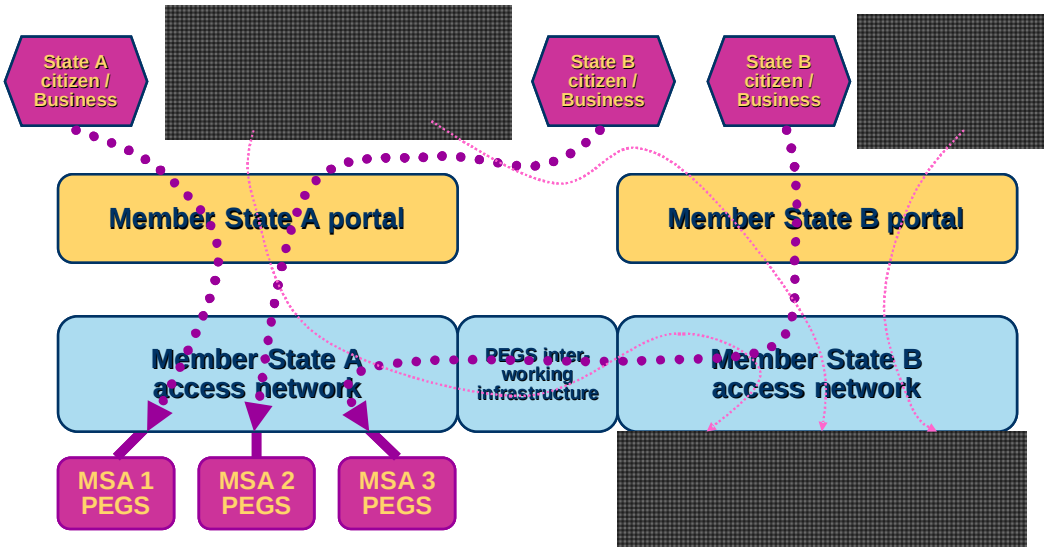

Figure 4 Working of National Services

Typically a national service is completely capable to fulfil its objective both on behalf of its own citizen or business and on behalf of business or citizens from other Member States. Citizens and business from other Member States have a choice to access the service through either the access infrastructure of the Member State to which the service applies, or of the Member State where they reside. In the latter case PEGS inter working services can optionally enhance the user experience, e.g. by providing language translation.

4.8.2 Communal Services

The typical working of communal services is shown in the next picture.

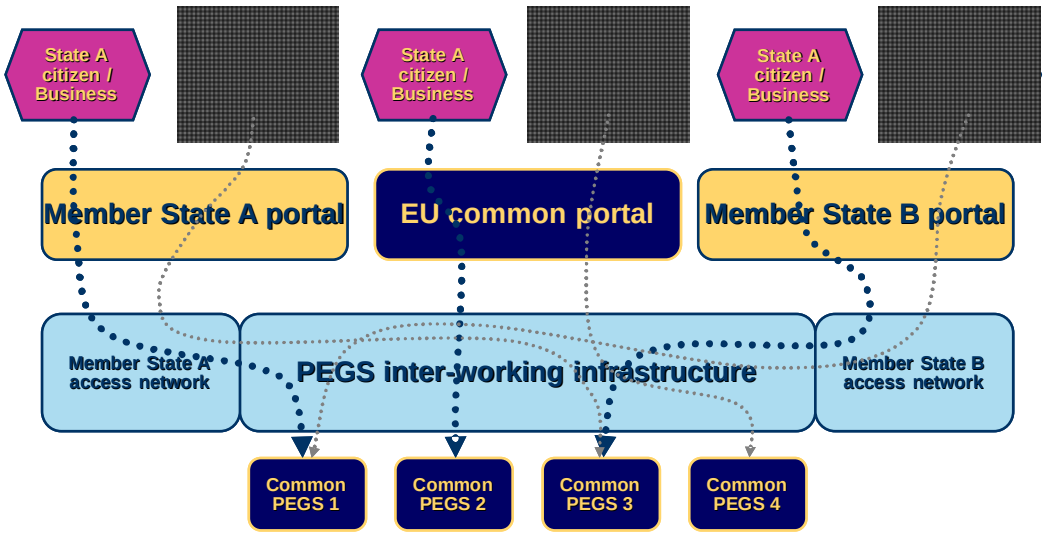

Figure 5 Working of communal services

This kind of PEGS is provided on an EU-wide scale on behalf of all citizens or business in all Member States. Typically, the citizen or business may have choice of accessing this type of service either via his national portal, a different national portal or

a common European portal. In either case the PEGS inter-working infrastructure can provide supplementary services like translation.

Like in the case of national services, communal services are complete, in the sense that they can fulfil their purpose without involvement of any MSA.

4.8.3 Supplementary Services

Supplementary services do not on themselves fulfil e-Government services, but can help enabling a wider audience for existing e-Government services. In particular it can make existing e-Government services accessible for citizens and businesses from other Member States. This is visualised in the next picture.

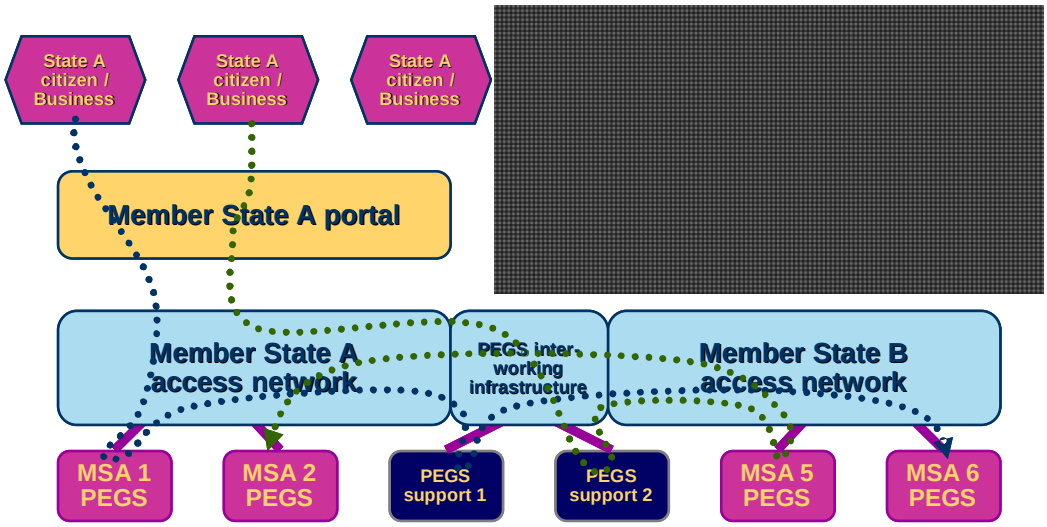

Figure 6 Working of Supplementary Services

In addition it can support services that require the cooperation between MSAs in multiple countries. Supplementary services can be provided through the inter-working infrastructure (as shown in Figure 6), by either of the member states involved in a service, or by an independent third party.

4.8.4 Inter-working services

Inter-working services do not generally interact with citizens or business in Member States, but can support the co-operation between MSAs. See next picture. Inter-working services come into play when direct communication between MSAs is not meaningful. Inter working-services typically support incompatibilities between semantics and/or business processes in the involved MSAs.

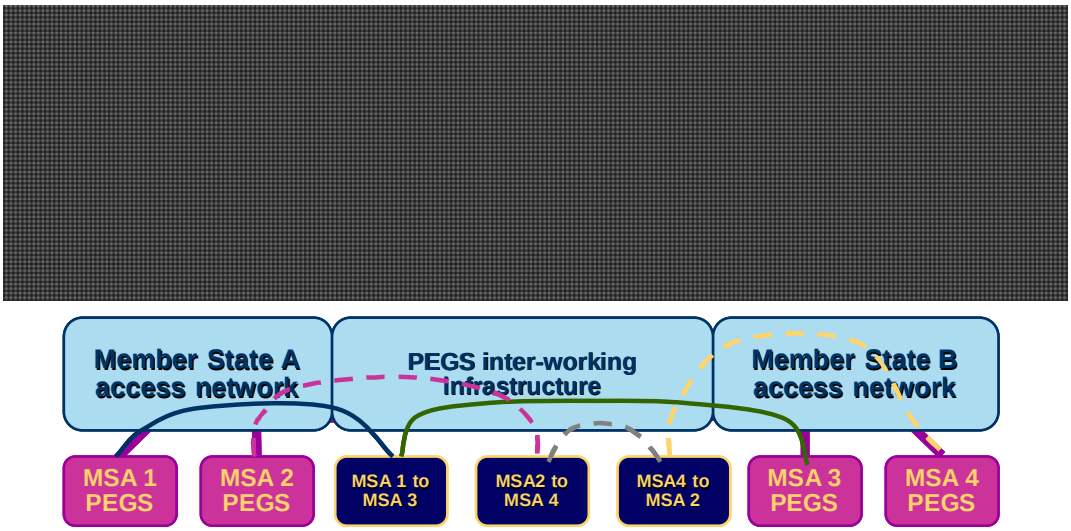

Figure 7 Inter-working services

Inter-working services can be part of the inter-working infrastructure or can be independent services provided through the inter-working infrastructure.

5 LOGICAL ARCHITECTURE

5.1 ALTERNATIVES AND PARADIGMS

In chapter 4.1 the requirements are described that Member State administrations will have to enable the support of government services for businesses or citizens from all countries in the European Union across Member State boundaries. Depending on the technical nature of the PEGS at hand and the differences between national or sub national implementations, this inter-working of PEGS can be solved in different ways. In the European Interoperability Framework (EIF) three levels of inter-operability are described. The following description is consistent with that description, but starts with a trivial case not described in the EIF. These descriptions detail the nature of the inter-working in various cases, but do not make assumptions about who implements which inter-working mechanisms where. It also does not make any assumption about who is responsible for instantiating, managing and operating such inter-working mechanisms.

In many cases MSAs or their governments have a choice in the approach of inter-working as discussed in section 4.1. In the development of a solution for specific PEGS two paradigms can be considered that represent alternative approaches:

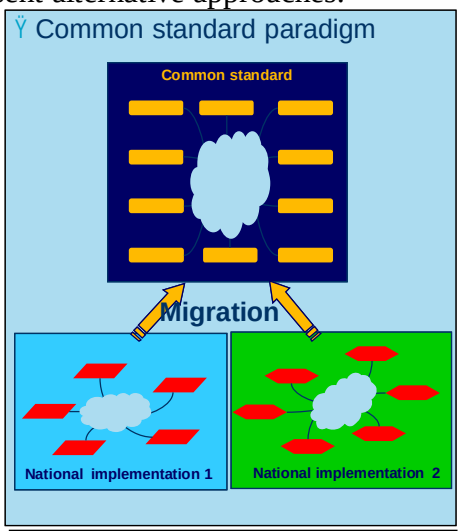

Figure 8 Common standard paradigm

1. Develop or apply a Communal guideline that in its most extreme form requires PEGS in all participating Member States to adopt common procedures, common semantics and common data formats. This approach is called the ‘common standard paradigm’ and results in the applicability of the “trivial-interoperability” model. This paradigm has the following characteristics:

    a. National operation may have to be changed to become in line with the common standard. Depending on the type of PEGS this may involve adaptation of national legislation. Subsequently a technical migration from existing national implementation towards a Communal implementation will be required. In practice this will result in elapsed lead time of many years.

    b. Single implementation in each Member State. This creates economies of scale in ICT implementations both within the involved administrations and for business and citizen having to interact with these administrations.

    c. May be in conflict with subsidiarity principle, by creating a tendency for centralised solutions. In combination with a drive towards cost saving,

this paradigm promotes a ‘one size fits all’ approach which enlarges the distance between citizens and government.

2. Leverage existing implementations and best practices that in its most extreme form implies that different business processes, different semantics, different languages and different technologies in various Member States are tied together by what is called the ‘mutual virtual representation’ paradigm. Each administration creates a kind of e-embassy at another administration with which it has to inter-work and vice-versa. This e-embassy will be fully adapted to the local best practices in the target administration environment. This paradigm has the following characteristics:

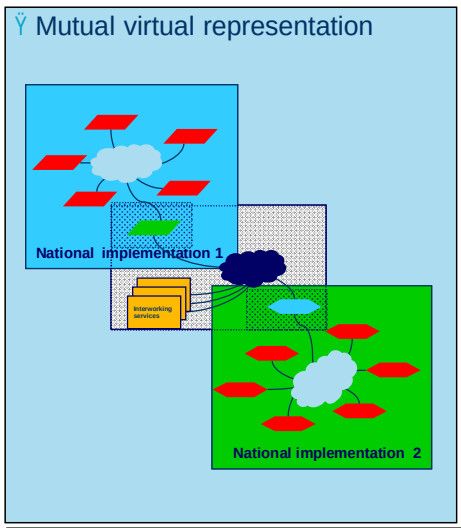

Figure 9 Mutual virtual representation

   a. Can be implemented bilaterally or multilaterally. Any group of administrations can implement this solution. Other administrations can join at their own pace

   b. Preserves national implementation. It usually does not depend on adaptation of national legislation and can therefore be started immediately. It also does not require national implementation to be changed and therefore does not have a complex migration path.

   c. It fully recognises and exploits decentralised solutions and therefore is favoured by the subsidiarity principle. The flipside of this coin is the tendency to have many different solutions for the same type of PEGS inter-working. In the worst case every participating administration must represent itself differently at any other participating administration. In practice it will not be that bad as the number of incompatible different solutions in most cases will be far less than the number of inter-working administrations.

   d. The operation of an ‘e-embassy’ will require additional inter-working services with additional governance and associated cost.

It is quite feasible that a group of administrations opt for a Communal solution for a certain PEGS, whereas others implement an inter-working solution with this group based on the ‘mutual virtual representation paradigm’. It also is possible that a group of administrations start with a solution based on the ‘mutual virtual representation’ paradigm, and work on common specifications in parallel with the objective to move towards the ‘common standard’ paradigm in a later stage.

5.2 DETAILED INTER-OPERABILITY ARCHITECTURE DESCRIPTIONS

This section describes solutions for the inter-operability types described in the EIF (ref. (3)). The solutions are ordered in increasing technical complexity.

As explained in section 5.1 the technically simplest inter-operability solution is the solution where MSAs can inter-work without a 3rd party gateway. To provide this standardised interface, any required conversion, transposition or representation has to be organised inside a MSA. Conversely, the technically most complex inter-operability scenario supports the situation with minimum technical impact on the MSAs. This other extreme assumes a gateway to overcome all differences at procedural, semantic and technical level. The current architecture provides for the coexistence of four inter-working scenarios in order to balance the effort to enable inter-working between MSAs on one hand and to design and implement the gateways defined by this architecture, on the other hand.

5.2.1 Trivial interoperability

The technically trivial situation is called “transparent or trivial inter-operability”.

This situation applies in cases where, mostly by virtue of European Union wide common specifications and standardisation, administrations within Member States, can directly exchange messages (see next picture[8]). This solution supports the 4th class of requirements as described in section 4.1.1.

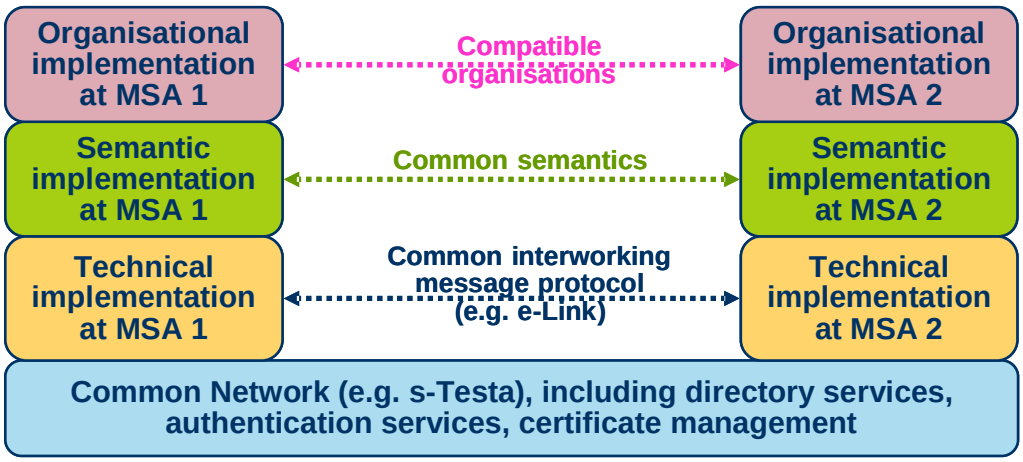

Figure 10 Trivial interoperability

I.e. a message sent from one MSA to the other MSA can be processed without conversion, adaptation, etc. The content of the message must have the same meaning in both MSAs and the role of the message in the business processes at both MSAs also is the same. It is assumed that the transport infrastructure provides the appropriate security services:

- Assure that the communicating MSAs have mutually authenticated themselves[9]

[8]] The picture shows the inter-working of 2 MSAs (bilateral inter-working) but likewise applies to any higher number of MSAs.

[9]] Some public, or lowly classified information can be sent without strong authentication applied

- Assure that the integrity and confidentiality requirements of the message are met
- If the message requires non-repudiation, assure that the sending and reception of the message by both MSAs is properly logged and time-stamped. Any required digital certificate to be used is up to the MSAs, however the transport infrastructure can provide a certificate as a trusted 3rd party.

The simplest security implementation for this case is modelled in the next picture.

Since both MSAs exchange messages using a common standard, there is no requirement for a concept like middleware[10]. Assuming that there is a direct (authenticated) connection between the MSAs (at least for the duration of the message[11]) there is also no need for intermediate store and forwarding nodes (message transfer nodes, like e-mail nodes), however if the required service level for a specific PEGS is compatible with asynchronous transport, it is fully acceptable to use a transport infrastructure with store-and-forward nodes.

To maintain the security context between MSA 1 and MSA 2 when store and forwarding nodes are implemented in between, the double envelope approach as described by the e-Link pilot may be used.

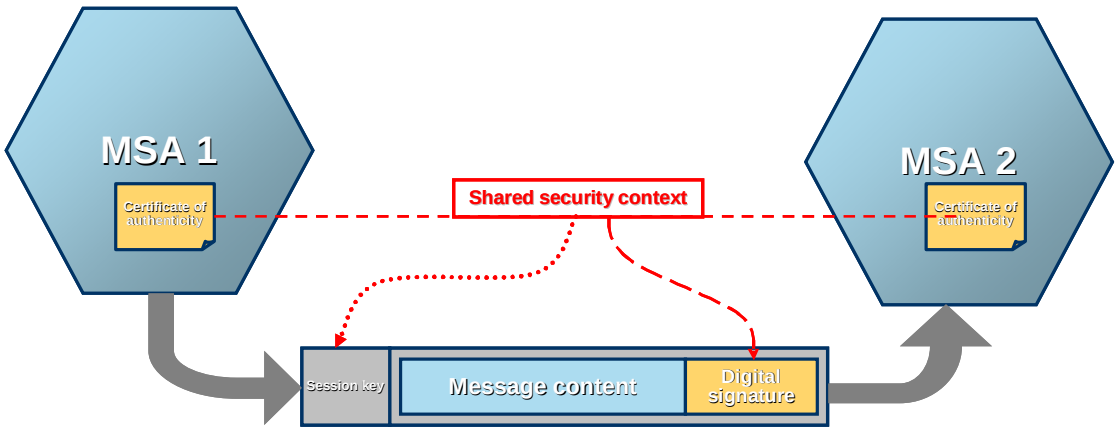

Figure 11 Simple trivial interoperability implementation

The only difference with the situation that both MSAs are in the same Member State is that for this kind of PEGS a Europe-wide message transport infrastructure (data network) is required, whereas in the national equivalent case, a national message transport infrastructure would be adequate.

In the “trivial inter-operability case” MSA1 and MSA2 are assumed to be communicating directly. Therefore any business state information of MSA1 and MSA2 is entirely the responsibility of MSA1 and MSA2 themselves[12]. The common network

[10]] The architecture does not require the MSAs to inter-work by means of middleware. If the PEGS already use or need middleware on a national level, this trivial case asserts, that the respective middleware implementations can be easily tied together, without additional logic in between, except for network transport

[11]] Typically administrations exchange a series of messages that together constitute the implementation of a business transaction.

[12]] Or their respective national middleware layers when applicable

has no recognition of any business state. The common infrastructure does however have knowledge about the connectivity status of all MSAs.

From an architectural point of view there is no limit to the bandwidth that is available between MSA1 and MSA2, so the scalability of the implementation is unlimited by architectural constraints

This "transparent inter-operability" can be considered as a trivial case of the next class, and therefore is not described separately in the EIF. In the rest of this document this case will be referred to as "trivial inter-operability".

5.2.2 Technical interoperability

The more general case is called "technical inter-operability" and is visualised in the next picture[13]. This solution satisfies the 3rd class of requirements as described in section 4.1.1. MSAs are assumed to be capable of exchanging messages by means of a "technical gateway", because they operate similar business processes and have common semantics to describe the various business objects relevant to the MSAs. The gateway must be capable of converting messages into different formats and protocols,. as supported by the respective MSAs.

Conversion services include all sorts of reformatting, language conversion, transliteration between Greek, Kyrillic and Latin alphabets. Other technical conversions, like network protocol conversions, units and currency conversion and message segmentation and reassembly of large messages can also be supported.

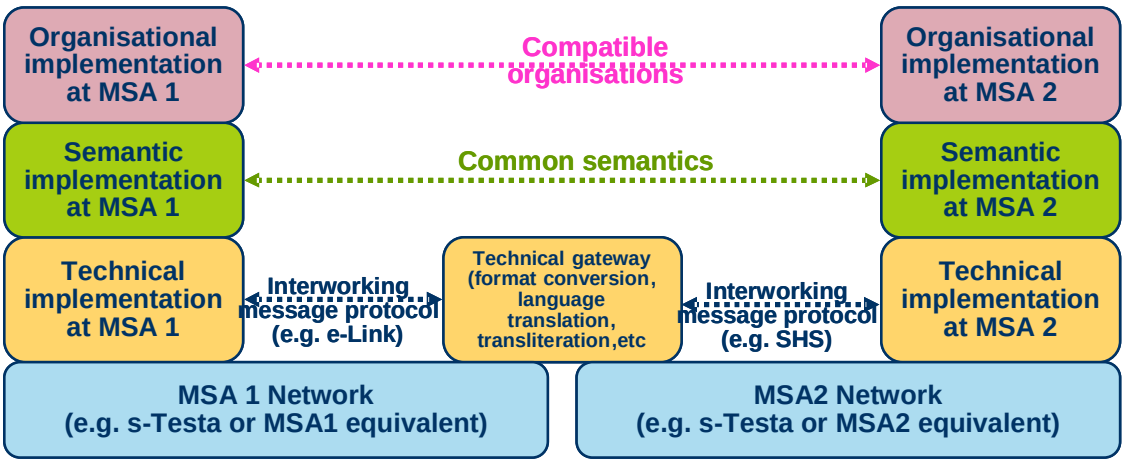

Figure 12 Technical Interoperability

The message must have the same ***content*** in both MSAs and the role and meaning of the message in the business processes at both MSAs also is identical. The "technical gateway" does not (need to) understand the meaning of the message; therefore any language translation is limited to 'stupid' translation, i.e. simple substitution of words or standard phrases using a static dictionary. From the above it can be guaranteed that the conversion applied by a technical gateway is fully reversible and symmetric, i.e. translation from MSA1-format to MSA2-format and back to MSA1- format will always return exactly the original message.

[13]] The picture shows bilateral inter-working but also applies for multilateral inter-working

Sealed message content that cannot be accessed by the technical gateway cannot be converted, and therefore must be understandable to both MSAs. This feature must be used by the MSAs to exchange digital signatures. Any essential information that cannot be understood by both MSAs without any conversion, translation, adaptation, etc will be converted by the technical gateway, or else the technical inter-operability case does not apply.

The technical gateway must share a security context with the sending and receiving MSA in order to be able to convert the content into the expected format. This also requires that the technical gateway must authenticate itself to both MSA1 and MSA2.

Since from a business perspective, the technical gateway is not the source or sink of any messages, just a relay, it is not necessary that MSA1 and MSA2 authenticate themselves to the technical gateway. They do need to authenticate each other! Apart from the involvement in the security implementations of both MSA1 and MSA2 the technical gateway is "stateless" (has no memory)[14] and is transparent to the business processes being executed between MSA1 and MSA2.

To validate the integrity of a translated/converted message, both MSA must trust the technical gateway, which therefore has to be certified. The technical gateway must be capable to validate and generate digital certificates that are exchanged with both MSA1 and MSA2. In addition MSA1 and MSA2 need to establish integrity management on the basis of a common secret (session key or challenge/response scheme) that is independent of the formatted content of the message, but will be derived from the identity of the technical gateway[15] (without the gateway itself being capable of verifying that). The next picture models the secure message transfer between two MSAs.

[14]] Having no knowledge about business states of MSA1 and MSA2 does not preclude the technical gateway to have its own internal state diagram for the operation of message transport with MSA1 and MSA2 independently.

[15]] MSA2 must have a way to validate that it received the converted message form the same gateway that MSA1 sent it to. Because that gateway is trusted by both MSAs, it can be assumed that the converted message is equivalent to the original.

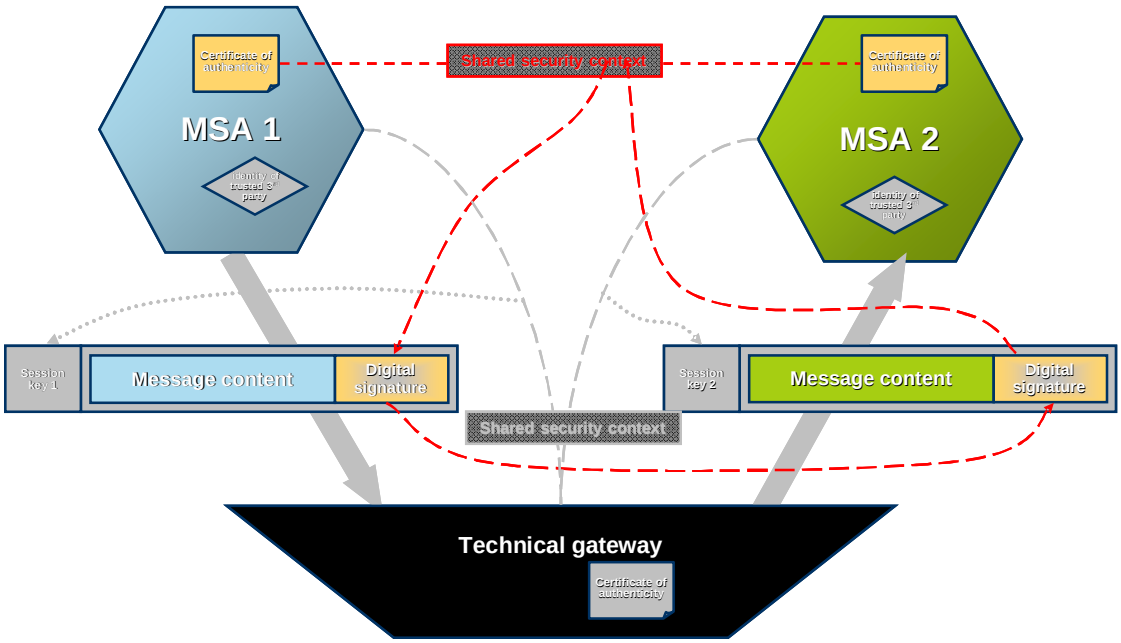

Figure 13 Technical gateway

The technical gateway exchanges messages with both MSAs[16] via either the same or a different message transport infrastructure, at least one of which must have Pan-European geographic coverage. Between the technical gateway and each of the MSAs "trivial inter-working" is assumed; i.e. the technical gateway inter-works with each MSA by using the formatting, language, code-table and segmentation options that apply to that MSA. The trivial inter-working between the technical gateway and each of the MSAs may be different with respect to any or all of the following[17]:

- Data-communication protocols
- Character set / code page
- Language
- Units and currency
- Message structure and data formats

The technical gateway is transparent for semantics and organisational differences or similarities.

The technical gateway can be implemented anywhere, either as a single instance or as a distributed system. When multiple instances of a technical gateway are implemented, the total collection of instances must support all message formats, codepages, languages and segmentation options that are required by the MSAs. Each one of them only needs to support a subset.

[16]]The gateway can be implemented bilaterally (with 2 sides) or multilaterally (with n sides, n>2). In the latter case it also supports one-to-many interaction types, where each of the destinations can have its own combination of data-communication protocols, character set/codepage, language, units & currency and message structure and data formats

[17]]When all of these are the same, the technical gateway is not needed, and "trivial inter-working" is applicable

It is possible to use multiple technical gateways in tandem configuration (cascaded)[18] to overcome the situation that none of them supports the direct transformation between source and destination format / character-set / language. In this case each of the technical gateways must be trusted and therefore authenticate themselves independently to both MSA1 and MSA2. The end-to-end message integrity then will be based on a common secret between MSA1 and MSA2 that must be derived from all of the identities of the technical gateway instances in between and the agreed sequence of using them.

From an architectural point of view there is no limit in the bandwidth available between MSAs and the technical gateway, and there are no restrictions on deploying parallel gateways to increase the available capacity. Since the technical gateway has no awareness of any business state information of MSAs, it has no affinity with specific exchanges between MSA1 and MSA2, i.e. when multiple messages have to be exchanged between MSA1 and MSA2 each message can be independently processed by any technical gateway or set of gateways. Of course every instance of a technical gateway needs its own security certificate.

5.2.3 Semantic interoperability

The next more complicated case is called “semantic inter-operability” and is visualised in the next picture[19]. In this case it is assumed that MSAs have similar business processes but do not use the same semantics to describe business objects. They may or may not use the same message formats, but because they communicate different business objects, this is of lesser importance.

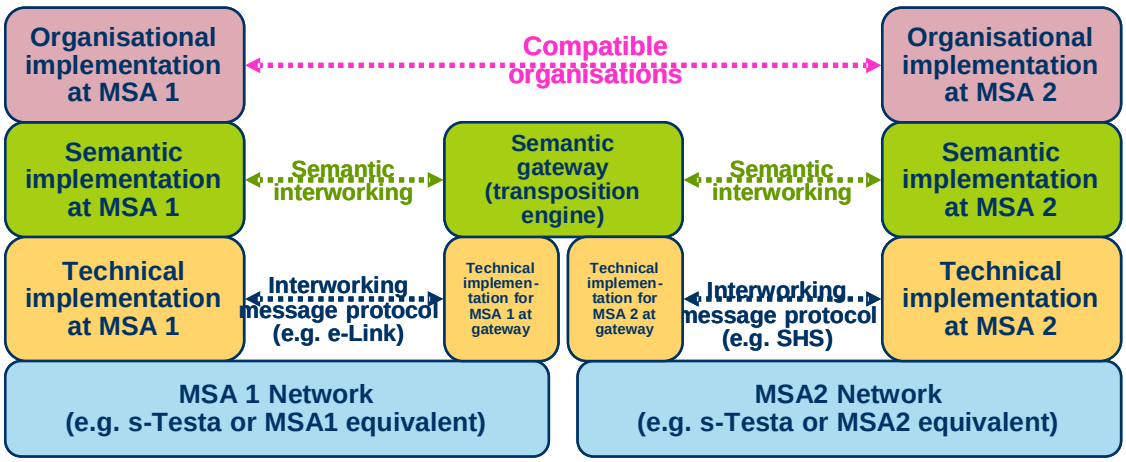

Figure 14 Semantic Interoperability

In line with the EIF, this case describes the situation where simple translation and reformatting of the message is not sufficient to make it understandable for the target

[18]]If for example the direct translation between Greek and Estonian is not available in any technical gateway, it is possible to have a translation into e.g. Portuguese in between

[19]] The picture shows bilateral inter-working but also applies similarly for multilateral inter-working

MSA[20]. Therefore a semantic gateway is required which can automatically discover and collect additional data, potentially from other sources, to build a message that has the same ***meaning*** and is a valid replacement for the message from the originating MSA in the actual situation. This solution supports the requirements for the 2nd class of inter-operating MSAs, as discussed in section 4.1.1.

Whereas the meaning of the message sent by one MSA is equivalent to the meaning of the message received by the other MSA, the exact content does not have to be directly related, and the potential difference in format and language therefore is irrelevant. The semantic gateway also supports more complex cases of languages translation, i.e. free format text translation, and more generally anything that a sworn interpreter could translate. Although the semantic gateway is symmetric on a semantic level (i.e. a message transposed from MSA1-semantics into MSA2-semantics and back to MSA1-semantics will give a message with identical meaning) it will not regenerate the original message, but just a compatible/equivalent message.

In order to fulfil its objective the semantic gateway will have access to context data both in Member State 1 and Member State 2, as well as to other kinds of data, including metadata translation tables.

The semantic gateway shares a security context with both MSAs[21] and must authenticate itself to both MSA1 and MSA2. The semantic gateway maintains process or transaction states, as well as "metadata translation tables" and therefore must be capable to act as agent on behalf of the other side. Therefore it is required that both MSA1 and MSA2 authenticate themselves to the semantic gateway. The security context of the semantic inter-working is visualised in the next picture.

[20]]An example to illustrate the difference between a technical inter-working and semantic inter-working is illustrated by the following case: The business object 'drivers licence' can be technically translated into 'Führerschein' or 'rijbewijs' or 'permis de conduire' without any knowledge of the meaning of either word, just by looking up a table and replacing the word.
If the classification of drivers' licences however is different from one country to another, it can be case dependent whether a class "C" 'drivers license' in one Member State (valid for vehicles > 3500 kg) corresponds to a class "II" (valid for vehicles < 7500 kg) or a class "III" (valid for vehicles > 7500 kg) 'drivers license' in another Member State. The semantic gateway has the capability to provide the correct substitution in either case, by identifying the difference in classification and querying the weight of the implied vehicle or by applying business rules to determine which substitution should be selected in each specific case.

[21]]It is assumed that, since MSA1 and MSA2 both belong to the EU, a common trusted 3rd party can be agreed on that will provide the common security context needed for implementation of a semantic gateway

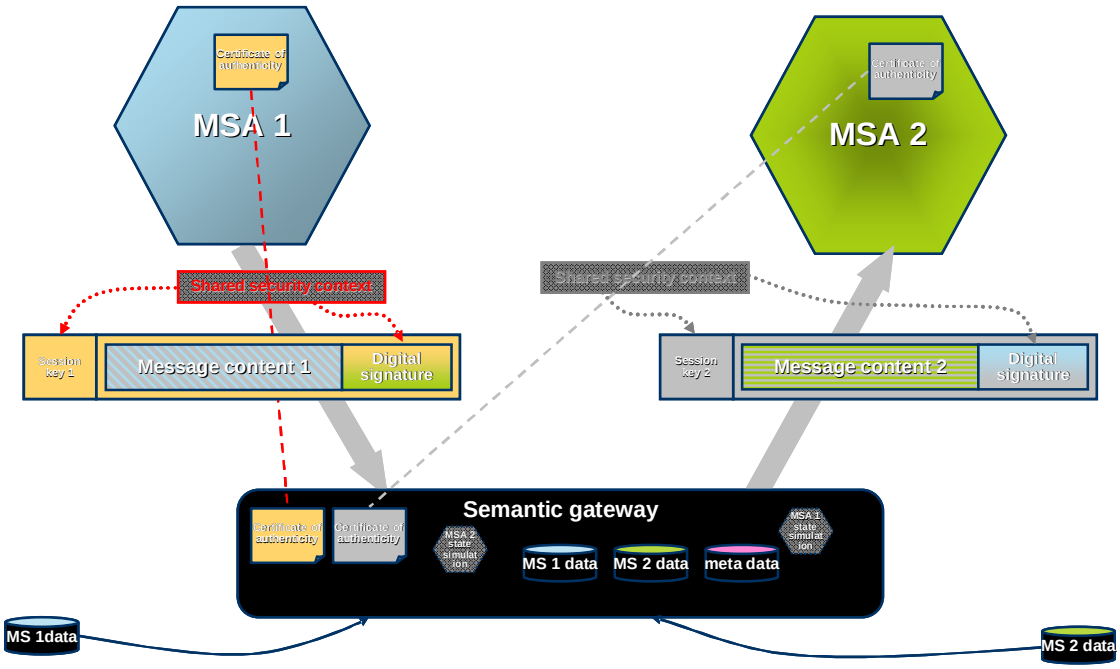

Figure 15 Semantic gateway

The mutual authentication and integrity management of a message between MSA1 and MSA2 also is more complex than in the case of a technical gateway. The proposed architecture involves two separately secured messages, one between MSA1 and the semantic gateway, and a different between semantic gateway and MSA2.. It is suggested that MSA1 includes some data about MSA2 to generate a digital signature, that the semantic gateway creates a reverse transposition of this data into the MSA1 taxonomy, and subsequently uses the result to generate the digital signature to be passed to MSA2.

Semantic gateways do not have the intelligence to operate business processes, but mimic business state changes on either side to the other. In order for these state changes to be meaningful, it is required, that both MSA1 and MSA2 have implemented the same or a compatible business process.

Semantic gateways can be cascaded with technical gateways on either side without restriction (see also section 5.4.2). The description of the technical inter-working then applies to the interaction between the semantic gateway and a MSA. It is also possible to have multiple semantic gateways to operate in series, but it is never necessary to use more then two semantic gateways in series[22]. The interaction between semantic gateways will be a case of trivial inter-working. In its operation there is no difference between a distributed implementation of a semantic gateway and two semantic

[22]] The assumption is made that, in order to develop a semantic gateway, a European Reference Taxonomy will have to be developed. Then a semantic gateway can always transpose between Communal reference taxonomy and the non-standard taxonomy of a Member State, or Market Sector. This assumption is supported by the observation that the number of different taxonomies within the EU is far less than the number of languages, message formats, characters, etc. Therefore, with a maximum of 2 transpositions in series any-to-any transposition can be supported. It is recommended to have one system architecture for the implementation of the semantic gateway.

gateways operating in series. Therefore it is recommended to have one system architecture for the implementation of the semantic gateway.

Semantic gateways can be function-limited to specific business areas[23]. If messages are subsequently passed through multiple different function-limited semantic gateways, the order of the semantic transpositions may be relevant, i.e. transposing vehicle semantics and subsequently driver semantics may give a different result than transposing driver semantics and subsequently vehicle semantics in the same context. This is caused by the fact that the 2nd semantic transformation of a message may find a different context, since context may have been modified as a result of the1st semantic transposition.

In combination with the symmetry property described earlier in this section, this means that meaning will only be recovered if reversal of semantic transpositions is treated as a stack (LIFO –last in first out).

5.2.4 Organisational interoperability

The most complex interaction is called "procedural[24] or organisational inter-operability". This type of inter-operability is shown in the next picture[25].

In this situation the sending by MSA1 of a message of whatever kind is not sufficient to make a state transition in the business processes of MSA2 happen, i.e. a message resulting from a change of business state in MSA 1 cannot be handled by MSA 2 because the implied state transition is not defined in the corresponding business process at MSA2. Depending on the PEGS at hand the organisational gateway needs to have its own business processes[26] in order to enable inter-operability between MSA1 and MSA2. This solution fulfils the requirements that relate to MSAs of the 1st class of section 4.1.1.

[23]] A function limited semantic gateway will only transpose business objects within its functional scope. It is feasible to pass a message through multiple semantic gateways, each with a different functional scope, and each will transpose 'its' parts of the message. This kind of serial transposition is not considered 'tandem' operation as described in the preceding paragraph.

[24]] In the EIF this type of interaction is called organizational inter-operability. We prefer the term procedural inter-operability since it more closely refers to the kind of complexity addressed: administrations with different business processes to achieve the same goal.

[25]] Contrary to the technical and semantic gateways, the procedural inter-working by nature is bilateral only. It is feasible to have multiple bilateral procedural gateways implemented on a shared platform, so it resembles a multilateral gateway. There is however a fundamental difference. A multilateral gateway can support one-to-many inter-working relationships by implementing distribution and/or publish/subscribe mechanisms. A bilateral gateway only inter-works between a designated pair of MSAs.

[26]]A business process in a procedural gateway exposes on the MSA1 side the methods that MSA1 expects MSA2 to have and exposes on the MSA2 side the methods that MSA2 expects MSA1 to have. Invocation of these methods by MSA1 and MSA2, respectively invoke state changes in the business process of the procedural gateway. The logic of this business process is the reconciliation of the processes at MSA1 and MSA2.

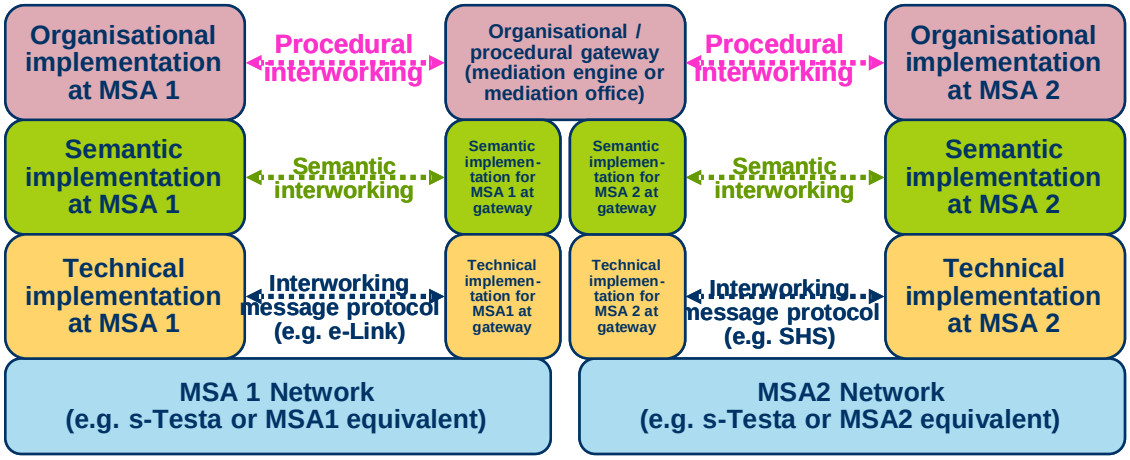

Figure 16 Procedural Interoperability

An example of such a gateway business process may include the initiation of financial transactions that are required by either of MSA1's or MSA2's business processes, or the sending of physical documents, or other objects. In many cases existing implementations at MSA1 or MSA2 are not capable to handle international payments, mostly because the field lengths and integrity checks for the payment data are customised to only handle valid national formats. Also it is possible that either side does not implement a payment interface at all, because the transaction is not charged in that Member State. In such a case the procedural gateway would initiate/handle a normal payment transaction(s) in national format as expected by either side, using account numbers of its own, and reconcile the financial positions resulting from that.[27]

The organisational/procedural gateway has extensive understanding of the business processes involved at MSA1 and MSA2 and must share the security context with both MSAs on the operational decision making level.

The organisational gateway acts as a kind of e-embassy between the MSAs. The organisational gateway fully represents MSA2 in the interaction with MSA1 and represents MSA1 in the interaction with MSA2. This also implies that a gateway of this kind exclusively "owns" each unit of work directed to it[28], has case affinity.

This type of interaction is visualised in the next picture. Procedural gateways are intelligent and can map multiple business processes on MSA2 side to a single business process on MSA1 side or vice versa based on the content including historic data about the other MSA (learning).

[27]]Using the transparency principle, it can be argued that services that are offered free of charge in a Member State, must be offered free of charge to all EU citizens applying for that service, and by consequence any payment required in other Member States for the same service, or for parts of the fulfilment of the service, must be allocated elsewhere. The procedural gateway would have the appropriate logic to allocate these costs, based on applicable agreements underlying the PEGS.

[28]]Parallel technical or semantic gateways can load-balance individual messages, or at least individual transactions, as they do not maintain context information about the work being passed thru it. The procedural gateway must store context information, since it cannot map transactions between MSAs.

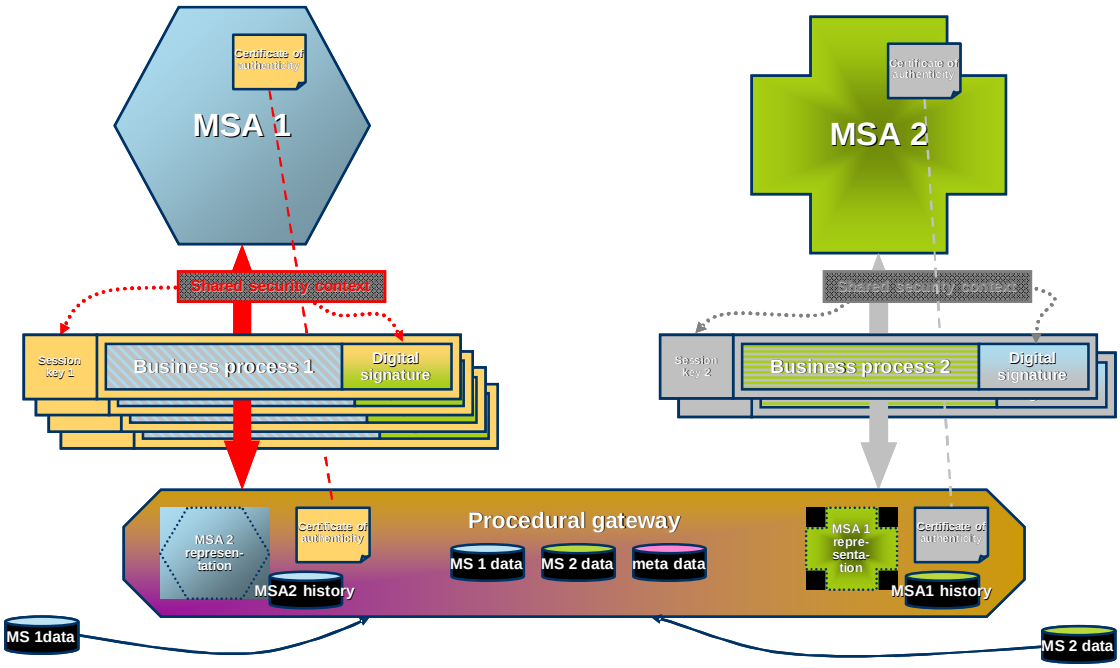

Figure 17 Procedural gateway

It is assumed that the procedural gateway builds up knowledge about the cases it handles and therefore becomes more efficient in handling specific business transactions between specific MSAs over time.

The implementation of the procedural gateway is based on bilateral agreements between a pair of MSAs or Member States with specifications for each PEGS to be supported. These specifications are the basis of the configuration data for the procedural gateway. Therefore it is not possible to cascade procedural gateways. The communication between the procedural gateway and either or both MSAs is preferably a case of trivial inter-working, although technical inter-working can be fully supported. If multiple MSAs within the same Member State use the same procedural gateway, based on a single bilateral agreement with another Member State, each of these MSAs independently can have trivial or technical inter-working with the procedural gateway. It is even possible that some of the MSAs connect to the procedural gateway via a semantic gateway, but not on both sides of the procedural gateway simultaneously[29].

[29]]If both MSA1 and MSA2 would communicate to the procedural gateway via a semantic gateway it is impossible to test the validity of the inter-working

The following table gives an overview of the combinations of MSA-procedural gateway communications that are supported or are not.

MSA1 - procedural gateway	*trivial*	*technical*	*semantic*[30]
MSA2 – procedural gateway			
Trivial	Yes	yes	yes
Technical	Yes	yes	yes
Semantic[31]	Yes	yes	**NO**

By definition MSA1 and MSA2 can communicate on procedural level using the procedural gateway, and each can communicate to the procedural gateway on all levels either directly or indirectly according to the above table. It is therefore irrelevant whether MSA1 and MSA2 share semantics, language, standard data format, and /or message transport networks. However, at least either of the transport networks must have Pan-European coverage.

5.2.5 Comparison table

This logical architecture does not assume that each of the solutions described in sections 5.2.1-5.2.4 will be implemented independently. It is assumed that for each type of gateway a separate business case will be developed.

The order of complexity suggests that each of these business cases only will show an acceptable ROI when the less complex gateways are justified also. It is therefore safe to make the assumption that a procedural gateway can be architected as an extension of a semantic gateway. Similarly, a semantic gateway can be architected as a superset of a technical gateway. Finally the technical gateway can be assumed to exist only when the requirement interconnecting network infrastructure (backbone) is available.

It should be kept in mind that the interaction modelling between MSAs, as described in the preceding sections, is not limited to back-office integration of e-government services, but applies to front-office (i.e. portal type) integration as well.

The following table summarises the differences between the various inter-working cases:

[30]]At least one instance of MSA1 in a Member State 1 must have a trivial or technical inter-working with the procedural gateway in order to have a reference implementation for the supported PEGSs

[31]] At least one instance of MSA2 in a Member State 2 must have a trivial or technical inter-working with the procedural gateway in order to have a reference implementation for the supported PEGSs

Characteristic	Inter-working types			
	Trivial	Technical	Semantic	Procedural
Defining characteristics				
business process compatibility	yes	yes	yes	no
common semantics	yes	yes	no	undefined
common communication protocol	yes	no	undefined	undefined
common message formats	yes	not required	undefined	undefined
common language and characterset	yes	not required	not required	not required
common units and currency	yes	not required	undefined	undefined
Gateway properties				
content awareness	no	no	yes	yes
business objective awareness	no	no	no	yes
delegated resposibility	no	no	no	yes
symmetric on data level	yes	yes	no	no
symmetric on content level	yes	yes	yes	no
symmetric on business objective level	yes	yes	yes	yes
security policy requirement	shared	common	compatible	undefined
secure message transport	transparant	trusted	trusted	trusted
secure authentication of MSAs	transparant	transparant	trusted	trusted
cascading of gateways	not applicable	yes	max 2	no (max 1)
MSA business state awareness	no	no	yes	yes
transaction management	no	no	limited	yes
context discovery	no	no	yes	yes
fully compatible in national context	no	no	no	yes
transparant performance	yes	yes	yes	no
performance degradation compared to national	no	small	moderate	undefined
case affinity	not applicable	no	no	yes
load sharing / unlimited scalability	yes	yes	yes	no
multilateral implementation possible	not applicable	yes	yes	no
distributed implementation	not applicable	possible	recommended	mandatory

5.3 SOLUTION LAYERING

In the modelling of solution alternatives in section 5.2 we assume that MSA1 in Member State 1 interacts with MSA2 in Member State 2. A more detailed description of the real situation provides the following possibilities:

- MSAx represents multiple Member States who have agreed on a common administration for a PEGS. This includes the case that an EU Institution represents a number of Member States[32] for a certain PEGS.
- MSAx represents one Member State with a centralised national implementation of a PEGS
- MSAx represents a region or smaller geographic part of a Member State with a decentralised nationally common implementation of a PEGS.

[32]] An example of such an institution could be the European Central Bank in Frankfurt, which represents 12 Euro-countries on monetary affairs, and which would have to inter-work with national central banks in the other Member States.

- MSAx represents a region or smaller geographic part of a Member State with multiple decentralised implementations of a PEGS.
- MSAx represents a business sector or group of business sectors. Other business sectors may be represented by other MSAs with different implementations
- MSAx represents a subset of possible lifecycle events in a Member State. In other situations a different MSA with potentially a different implementation may represent the PEGS in a Member State
- Legislation within a Member State defines that Businesses operating in a free or regulated market implement the PEGS on the basis of a concession. Multiple businesses within the same Member State may compete as MSA, each with its own, potentially different PEGS implementation

Whenever multiple MSAs within one Member State exist (according to any of the above cases) National e-Government Services (NEGS), similar to the PEGS, will need inter-working solutions according to the same model as described in chapter 4, and may have taken initiatives to create an architecture similar to the one described in section 5.2. So, for the realisation of NEGS, a Member State may have created:

- A national network infrastructure
- National technical gateways
- National semantic gateways
- National procedural gateways

The following picture gives an overview of the various inter-working cases for trivial inter-working:

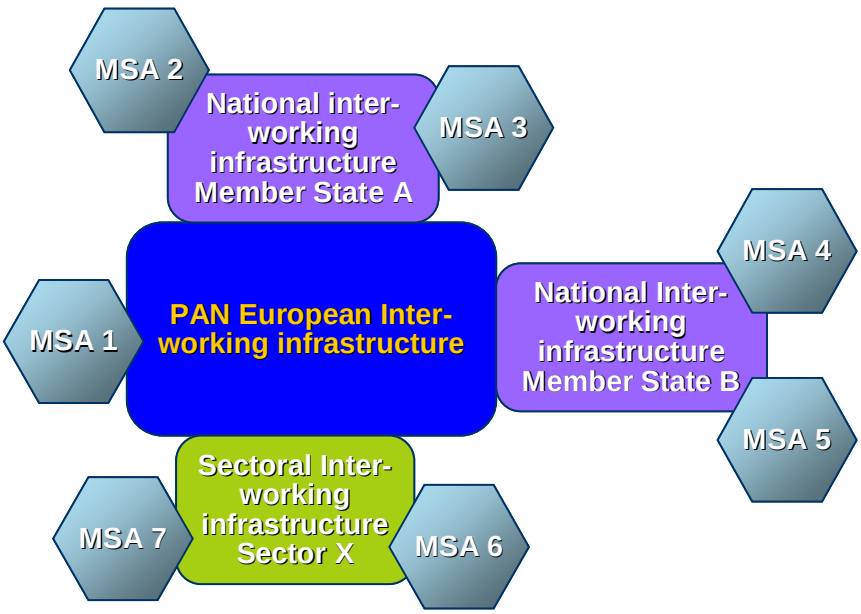

Figure 18 Trivial inter-working cases

In the above picture the following inter-working cases are considered in/out of scope:

In scope ?	MSA 1	MSA 2	MSA 3	MSA 4	MSA 5	MSA 6	MSA 7
MSA 1		Yes	Yes	Yes	Yes	Yes	Yes
MSA 2	Yes		**No**	Yes	Yes	Yes	Yes
MSA 3	Yes	**No**		Yes	Yes	Yes	Yes
MSA 4	Yes	Yes	Yes		**No**	Yes	Yes
MSA 5	Yes	Yes	Yes	**No**		Yes	Yes
MSA 6	Yes	Yes	Yes	Yes	Yes		**No**
MSA 7	Yes	Yes	Yes	Yes	Yes	**No**	

It is assumed that national or sectored initiatives in the area of network-infrastructure will provide collective connectivity for MSAs from the same Member State or from the sector. The next picture shows inter-working cases when using technical gateways:

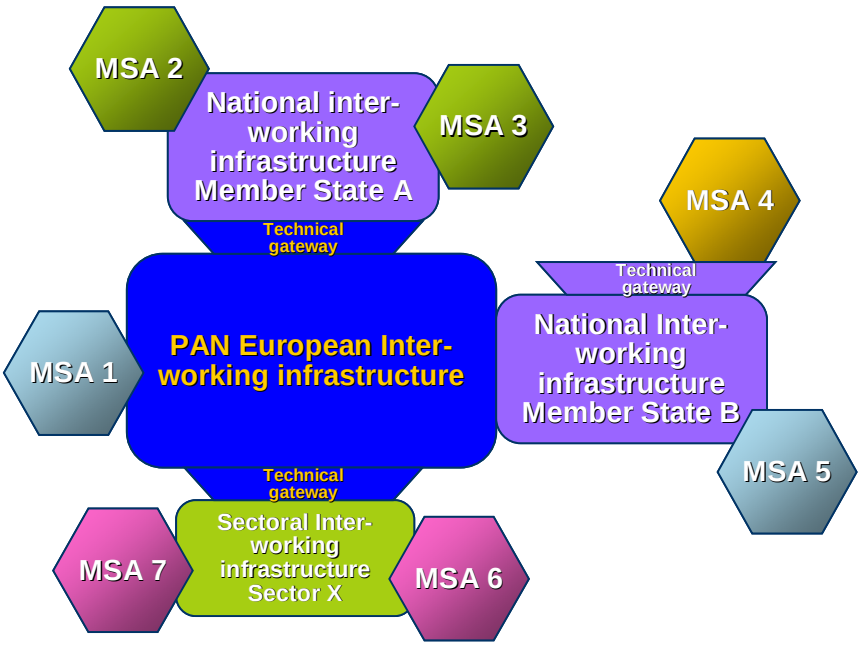

Figure 19 Inter-working using technical gateways

The technical gateway needed to inter-operate with MSA 4 is out of scope, since it is also required for national inter-working between MSA4 and MSA5. It is assumed that the national authorities in Member State B will have taken adequate measures to provide inter-working with MSA 4 on a national level, and since MSA5 supports trivial inter-working with MSA 1, the technical gateway in Member State B will be a sufficient solution for inter-working between MSA 4 and MSAs in other Member States. In as far as technical gateways are implemented by means of middleware, the technical gateways that are in scope can be considered as a middleware of middlewares.

The next picture shows some inter-working when a semantic gateway is needed:

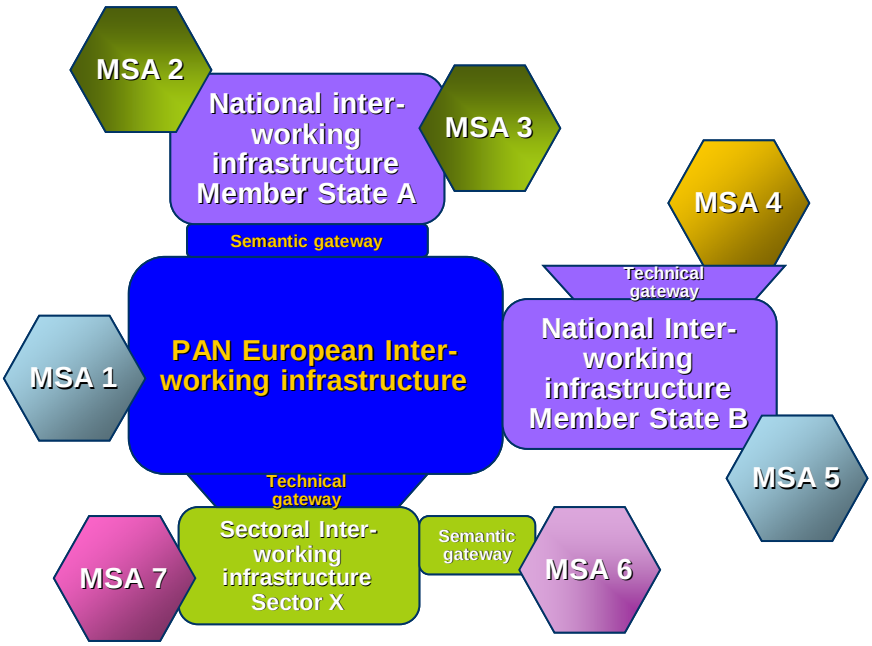

Figure 20 Inter-working when using semantical gateways

Similar to the previous case: the semantic gateway for inter-working with MSA 6 is considered out of scope, since it is also needed for inter-working with MSA 7, within Sector X, which has a sectored inter-working infrastructure in place. It is assumed that the semantic gateway available to enable inter-working between MSA 6 and MSA 7 within sector X will, in combination with the technical gateway between the sectoral inter-working infrastructure for sector X and the PAN European will enable inter-working of MSA 6 across the community[33].

The next picture shows some inter-working in case a procedural gateway is needed:

[33]] This assumption implies that Sectoral E-Governments Services (SEGS) utilise the full taxonomy required for PEGS and NEGS. If this assumption cannot be held, i.e. when a PEGS requires a wider set of transpositions then SEGS, the semantic gateway between MSA6 and the sectoral inter-working infrastructure for sector X, needs to be supplemented with a semantic gateway that provides the additional semantic transposition capabilities. This supplementary gateway would potentially be in scope of the PEGS inter-working architecture.

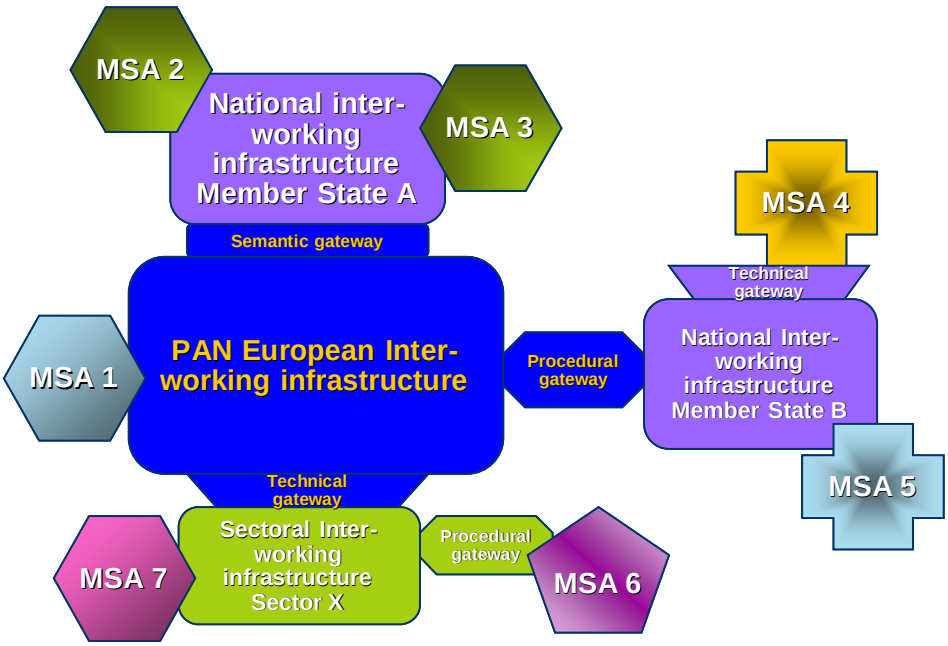

Figure 21 Inter-working in the case of a procedural gateway

In line with the previous cases, the procedural gateway between MSA 6 and the sectorial infrastructure is considered out of scope since it is also needed for inter-working within sector X with MSA 7. The following table summarises the inter-working cases of the last figure:

In scope	MSA 1	MSA 2	MSA 3	MSA 4	MSA 5	MSA 6	MSA 7
MSA 1		Yes, semantic	Yes, semantic	Yes, procedural	Yes, procedural	**Partly, technical only**	Yes, technical
MSA 2	Yes, semantic		**No**	Yes, procedural	Yes, procedural	**Partly, semantic only**	Yes, semantic
MSA 3	Yes, semantic	**No**		Yes, procedural	Yes, procedural	**Partly, semantic only**	Yes, semantic
MSA 4	Yes, procedural	Yes, procedural	Yes, procedural		**No**	**Not possible**	Yes. procedural
MSA 5	Yes, procedural	Yes, procedural	Yes, procedural	**No**		**Not possible**	Yes, procedural
MSA 6	**Partly, technical only**	**Partly, semantic only**	**Partly, semantic only**	**Not possible**	**Not possible**		**No**
MSA 7	Yes, technical	Yes, semantic	Yes, semantic	Yes, procedural	Yes, procedural	**No**	

5.4 HIERARCHICAL AND RECURSIVE IMPLEMENTATION

In the previous sections no explicit mention is made of the complexities which arise when the various gateway types, do not exist, or are not available when needed.

In order to fulfil a PEGS transaction in a specific case at a specific moment the following conditions can occur:

1. The remote MSA(s) which have to be involved to complete the transaction can be identified using the White Pages and is/are either capable of trivial inter-working or capable of inter-working by means of a technical gateway.
2. The remote MSA(s) which have to be involved to complete the transaction can be identified using the White Pages but is/are not capable to inter-work either trivially or by means of a technical gateway, and the subject of the inter-working is covered by one or more semantic gateways that can be found by means of the Yellow Pages service.
3. The remote MSA(s) which have to be involved to complete the transaction can be identified using the White Pages but is/are not capable to inter-work either trivially or by means of a technical gateway, and the subject of the inter-working is not covered by any of the semantic gateways that can be found by means of the Yellow Pages service.
4. The remote MSA(s) which have to be involved to complete the transaction cannot be identified, neither using the White Pages nor by means of Yellow Pages, but is known to exist. Potentially some of the Government Services addressed are manual processes (at some of the MSA(s).

5.4.1 Case 1: Straight inter-working

In this simple case the involved MSAs have been identified, are known to have common semantics and compatible processes, and any technical differences can be solved by any technical gateway that can be deployed. Apart from the additional process time required to apply technical conversions, the performance of the PEGS can be expected to be very similar to the corresponding NEGS.

5.4.2 Case 2: Semantic conversion

In this case the involved MSAs have been identified, but do not have common semantics. Depending on the business objects involved in the performance of the PEGS, the MSAs have to select and agree on a trusted semantic gateway that holds the capability to transpose the involved business objects. The identification of this semantic gateway can be by means of “yellow pages” or be known in advance.

It is not necessary that the selected semantic gateway can trivially inter-work with any of the MSAs. Within the semantic context between the semantic gateway and each of the MSAs, a technical gateway can be necessary. In order for this to be treated as a case of straight inter-working, all semantic gateways have to be listed in the “white pages”. This enables technical inter-working between the semantic gateway and the MSA. See next picture.

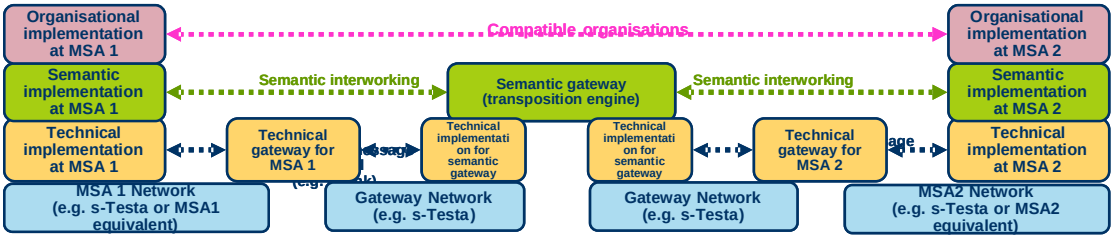

Figure 22 Semantic gateway using technical gateways

In a sense the technical inter-working is subordinate to the semantic inter-working. This allows for an overall design that plans deployment of semantic gateways totally independent of the deployment of technical gateways.

5.4.3 Case 3: Procedural mediation

In this case the involved MSAs have been identified, but do not have common semantics, and a search through the yellow pages has not revealed the existence of a suitable semantic gateway. As discussed in section 5.2.4 a procedural gateway is needed to enable inter-working between MSAs. The procedural gateway is identified as a NEGS in each of the Member States that have bilaterally agreed to operate a procedural gateway. The implementation of the NEGS in each of the Member States is outside the scope of this document, but will generally follow patterns similar to these described as trivial or technical inter-working.

Multiple Member States with compatible business processes for selected PEGSs can technically share a procedural gateway to another Member State[34] with different business processes. Within such a group of Member States with compatible business processes case 1 (without restrictions) and case 2 (with restrictions as explained in 5.2.4) can be applied.

5.4.4 Case 4: Incompatibilities between member countries

In this case the involved MSAs cannot be identified. A citizen or business to which this happens unfortunately has a problem that cannot be solved by this architecture. Until the involved MSAs have been identified by other means (external to the infrastructure, e.g. by hearsay or by reference to citizens or business with similar intent), it is not possible to execute any PEGS by whatever type of gateway.

It is however possible to create a procedural gateway to a Communal middleware environment without MSAs attached. It would be possible to publish a request of a citizen or business on this middleware, and wait for an extended period on a future subscriber. This would allow the queuing of a PEGS request for future Member States or for Member States that have, in accordance with the multiple speed principle, not yet implemented that type of PEGS. The desirability of such an approach in general and its applicability in specific cases needs further study.

[34]] or a group of member States with compatible business processes among them

6 PHYSICAL ARCHITECTURE

This chapter provides general implementation guidelines and provides the synthesis with the Technology trends document, ref. (2).

6.1 SCOPE

As already stated earlier, the analysis of technology and market trends is focused on those technologies relevant to the definition of an infrastructure for PEGS. It is worth expanding on the matters, and list more precisely what is in scope and what is out of scope such as to clearly position the present study, independently of any model architecture at this stage.

The PEGS Context:

The following IDA documents contain major guidelines and principles:

- § the European Interoperability Framework, ref (3) ;
- § the IDA Architecture Guidelines, ref (4);
- § the IDA eLink middleware, ref. (5).

The following terms: EuroDomain, LocalDomain, EuroGate are defined in IDA Architecture Guidelines.

The EuroGate is potentially more general than a PEGS interface node, hence the term **PEGS interface node** will be used to denote the functional parts (or sub-system) of a EuroGate that specifically handles PEGS flows.

Now taking into account a distributed implementation (because of the subsidiarity principle) that would take advantage from the pan-European IP network infrastructure (s-TESTA infrastructure), a distributed implementation of inter-working gateways would be represented as in Figure 23:

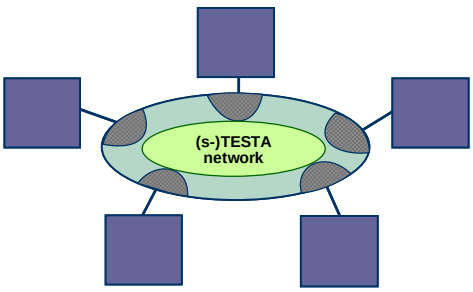

Figure 23 Implementation of inter-working gateways

Where the logical interoperability network boundary has been preserved; this is very important.

The key is then to consider that there are actually two boundaries:

- § The **Local Domain** boundary (as named in IDA-AG)
- § The **European Interoperability Infrastructure** boundary,

which can be identified on the following figure (zooming on a single administration, government agency or institution):

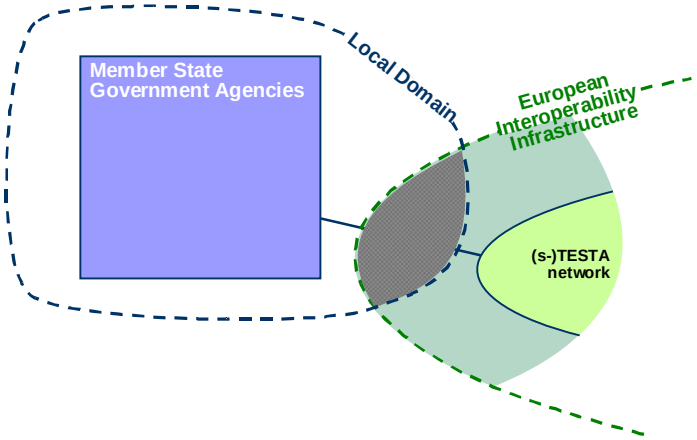

Figure 24 Definition of boundaries

Two interfaces must be considered, the interface between the PEGS interface node and the MSA on one side, and the PEGS-interface node with the (s-)Testa backbone network on the other side :

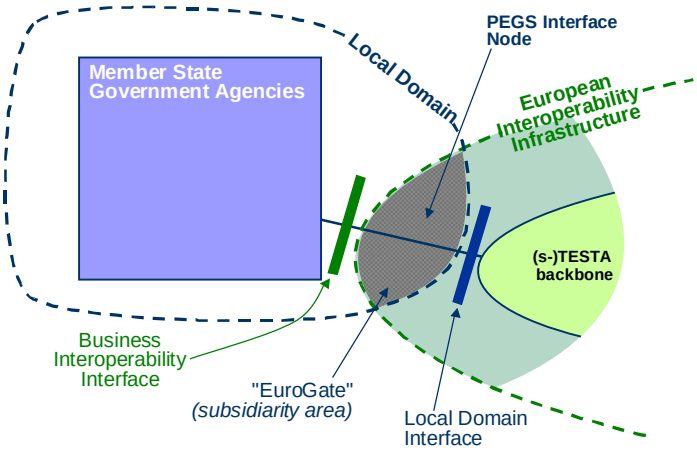

Figure 25 Interfaces

Depending on the type of gateway assumed or to be implemented the following possibilities exist:

- The PEGS-interface node is the full or distributed implementation of trivial inter-working. In this case the PEGS-interface node is just a router.
- The PEGS-interface node is the full or distributed implementation of a technical gateway. In this case the PEGS-interface node is a router with added light-weight application functions. The application functions running in a technical gateway node are implementations of the services described in section 4.4 and 4.5. There will not be much difference between a full or distributed implementation, except they will be

differently configured. In case of a full implementation, all MSAs to be interconnected must provide interconnection data to be configured into the interface node. In a case of a distributed implementation only one MSAs' interconnection data and those of a reference implementation will be configured into the interface node.

- The PEGS-interface node is the distributed implementation of a semantic gateway. In this case the PEGS-interface node will consist of a router with firewall and a set of application servers running the implementation of the services described in section 4.3-4.5.
- The PEGS-interface node is the distributed implementation of a procedural gateway. In this case the PEGS-interface node will be a more complex set of servers connected to a local network and made accessible by means of a router and firewall. A more detailed description of the configuration of this kind of interface node will be a deliverable of a more detailed architectural study of semantic and procedural gateways, based on more detailed specific information about typical PEGSs.

The next picture describes the interaction of a PEGS in more detail.

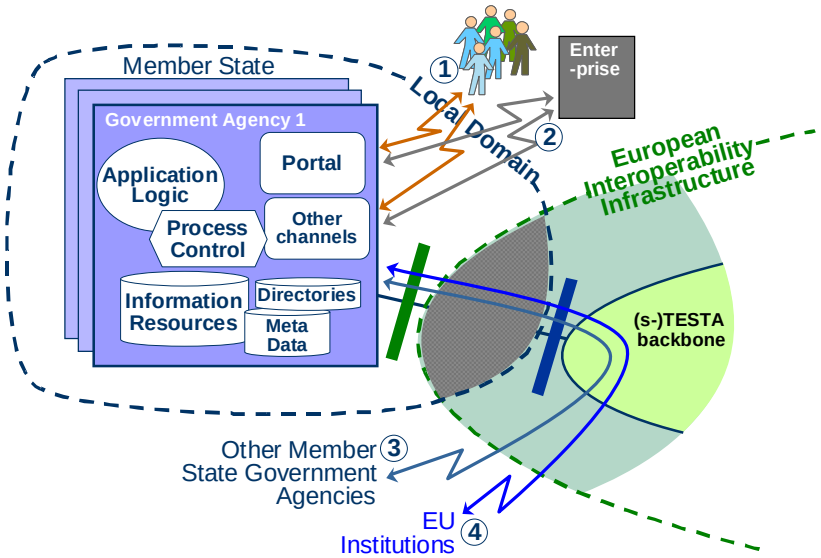

Figure 26 PEGS Interaction

EU institutions just stand like another government agency in another Member State. According to IDA principles, it is important to note that there will be no business application logic, information resources (business data, document stores…) standing in between two agencies or institutions beyond directory systems and other natural sources of reference data. In particular, it is not anticipated to host business process management engines within the common infrastructure. Every resource of business information and any piece of logic is located within the Local Domain of a Member State or the Local Domain of the EU. This implies that the procedural gateway must be fully implemented within the local domain of the EU.

One could have noticed that the figure only makes reference to the s-TESTA backbone and does not show the IDA eLink infrastructure. Indeed, the IDA eLink would be used too. However, it is not shown on the diagram for the following reasons:

- The implementation of eLink takes the form of additional components within the EuroGate area, else as part of the stack of a PEGS Interface node;
- Shared elements like directories are not illustrated elsewhere in this figure, hence the eLink directory (UDDI) is not represented;
- The present report is in essence open to all technology and market directions for what they are and where they go. Therefore, the loosest means to refine the scope are used, but not beyond. IDA eLink is defining a very precise middleware functionality compared to the s-TESTA infrastructure that provides managed IP network services.

Top down approaches are missing from the above list, and are just ongoing at this time. Assuming that these top down analyses will provide a formal catalogue of all PEGS that can be used by citizens and enterprises, we would still be left with a grey zone as shown in Figure 27 below, fitting in between the services as experienced by users and enterprises through various portals and communication gateways, core administrative applications and repositories operated by the Member States, and the communication infrastructures already largely described. All of that in compliance with the IT principles and governance rules cited above. This "grey zone" is represented in the figure below. This grey zone is the domain of the semantic and procedural inter-working.

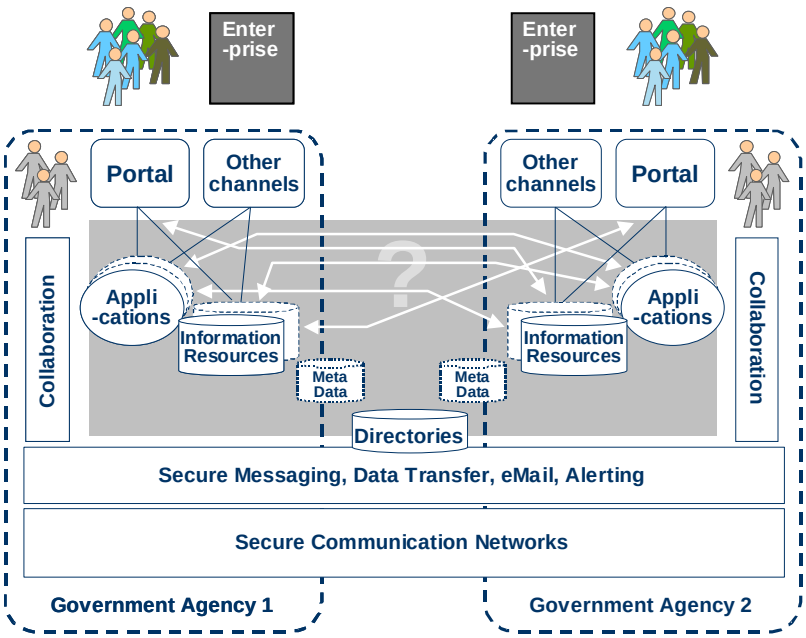

Figure 27

If the above Figure 27 is compared with Figure 26, one can immediately understand that the PEGS challenge is to **organise** all activities in support of the **processes** executed by users, enterprises, or administrations directly. On the one hand there is a need to place all individual government resources into a coherent pool (or global virtual application) for supporting PEGS. On the other hand, every resource is kept under control of the respective administrations and all coordination between these could only be executed via data communication through the networking infrastructures.

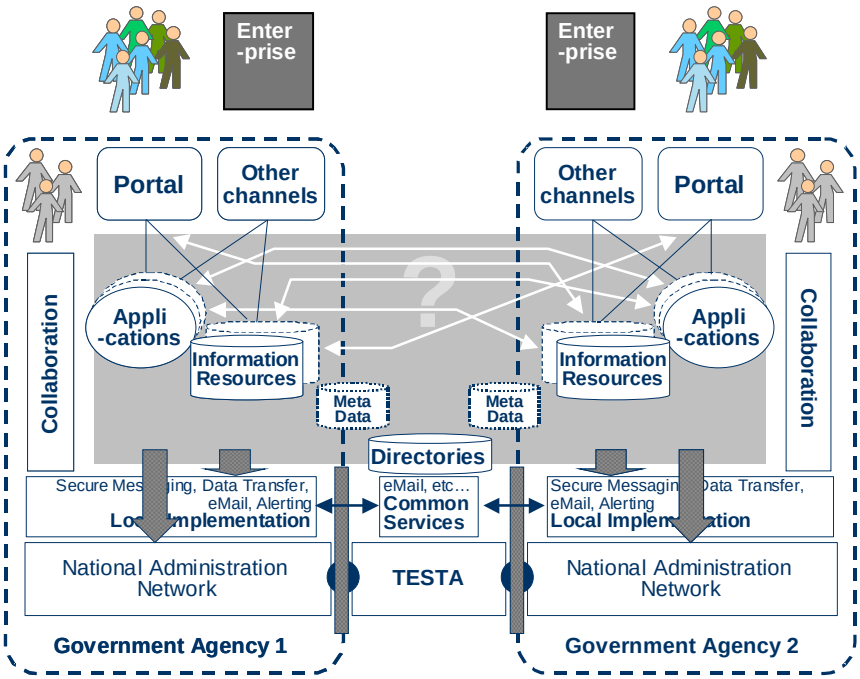

Figure 28

It is worth noting at this point that all functionality required for both network services (e.g. s-TESTA) and the value added services (e.g. eLink) can be enclosed into "black boxes" taking the form of network equipments and software components[35]. Interfaces to these equipments and components are then easy to identify and locate.

But the same reasoning cannot apply to deal with inter-operability in the "grey zone"! As will be seen, it is impossible to confine the functionality required for the interoperability of distributed processes and services into a 'box'. Indeed there are functionalities; indeed there are communication protocols and transactions at stake; but these are elements of a 'glue' rather than a 'box'.

Inter-operability will be constrained by the conformance to interaction schemes (e.g. a sequence of operations without defining the specific operations themselves), process templates, choreographies, ontologies but whose content could at no time be frozen. The concepts of sharing and conformance are moving from the domain of bits and bytes into semantics, meta-data and goals.

[35] Locally built or acquired from external sources.

Of course one can think of standardising some administrative procedures Europe-wide, and then mapping such standardised procedures[36] into precise interaction processes, with precise formats and error conditions[37]. Of course, a lot of extension points and options would have to go along. But how to deploy and maintain these standards at such a large scale? How much effort, even with a very good versioning system? How much time will it take before a common data model and standardised process could emerge - Europe-wide - for each administrative service to citizens and enterprises? [38]

6.2 REFERENCE SOLUTIONS

6.2.1 Trivial inter-working case

Trivial inter-working requires a secure and transparent transport-network between points of contact to the national transport network infrastructures in each of the Member States. As discussed in section 6.1, s-Testa qualifies as such. Based on population statistics from Eurostat, a first estimate is made of the percentage of access capacity to be allocated to each Member State[39]. Any bandwidth required by centrally managed Communal Services is assumed to be included in the bandwidth for each Member State.

[36] That also implies to harmonise data first!
[37] Modern process engines and web services would there be used as another (more efficient?) implementation technique, but not really as a new tool!
[38]]However, standardising data and semantics would always bear interest even with the newer approaches that deal with ontologies.
[39]]The figures do not exactly add up to 100% due to rounding

Figure 29 Access capacity by Member State

This initial estimate does not take into account that some Member States will implement decentralised access to the Pan-European backbone. It also does not take into account that businesses are likely to have a distribution that differs from population statistics.

6.2.2 Technical inter-working case

For the realisation of technical gateways a middleware solution is anticipated. In so far the MSAs are connected by means of national middleware solutions, the technical gateway can be seen as a middleware of middlewares.

It is anticipated that the technical gateways can be built from commercial off the shelve products (COTS)[40]. Further study is required to determine whether an open source middleware solution should be required and feasible.

[40]] If COTS products are considered for a first implementation, the Tibco Middleware suite can be considered as a point of reference to define more detailed requirements. Cisco Systems are about to announce hardware components with functionality suitable to implement remotely manageable technical gateways. Whether this product suite actually fulfils all requirements for a technical gateway is not determined in the present study

6.2.3 Semantic inter-working case

For the realisation of semantic gateways a more detailed architecture study is recommended. Current understanding suggests that this more detailed architecture study will be oriented around an enterprise content management (ECM) solution.

This ECM solution is likely to include a COTS ECM product[41]. Further study is required to determine what other components are needed to create a fully functional semantic gateway, and to what degree these components should be based on open source solutions.

6.2.4 Procedural inter-working case

For the realisation of a procedural gateway a more detailed architecture study is required. This study is likely to require two phases. In the first phase a generic procedural gateway solution is defined, which takes the detailed architecture of the semantic gateway into full account. The centrepiece of this domain level architecture is likely to be a case processing tool[42].

The 2nd phase would produce a more detailed architecture based on an intended list of PEGS and Member States for which procedural inter-working is required.

6.3 ACCESS TO PEGS

Access to PEGS will be based on portal technology. Three independent portals are required, for citizens, for business representatives and for civil servants respectively.

Each portal will define three layers of access.

The first layer of access provides all relevant public information and interactive services that are made available for anonymous access[43]. Personalisation can be provided by storing relevant service configuration data and interface customisations in cookies.

The second layer is assumed to store protected private data. In order to get access to this layer each user will be required to setup a personal user-id and password. Information stored in this layer is available to the user in all interactions with all PEGSs. However, the user decides when and where to provide this data to any PEGS. Whenever he does, the data he provides help fulfilling the one-stop shopping principle.

---

[41]] If COTS products are considered for a first implementation, the Hummingbird ECM product suite is a suitable point of reference for defining the detailed architecture of the semantic gateway, and based on that for the detailed requirements of the ECM component in that solution.

[42]] If COTS products are considered for a reference architecture for the procedural gateway, the Opalis product is a candidate for further analysis of the reference architecture. Further study is required to determine whether this products fulfils the requirements defined in this reference architecture, and whether an Open Source product should be preferred.

[43]] If access to these services is to be limited to the defined audience of citizens, businesses and administrations of Member States only, some extranet or intranet layer is required to separate these services from the open internet.

The third layer is assumed to require strong authentication of the user. Any data provided on this layer can automatically be shared by all PEGSs. This third layer is assumed to include all authentic sources of information. The data stored in this layer will always fulfil the one-stop shopping principle, including cases where information stored by administrations are not to the advantage of implied citizens or businesses.

The following picture visualises this three-layer approach.

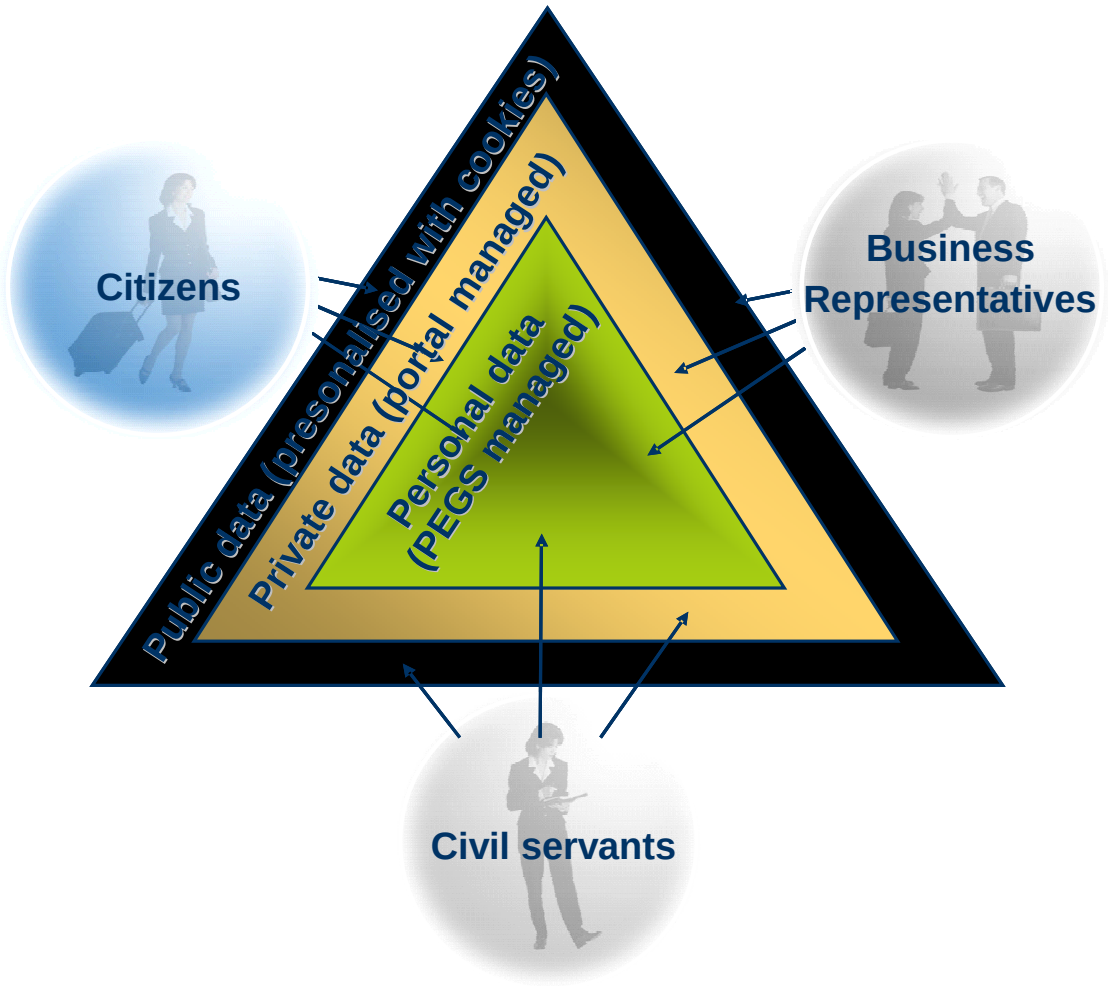

Figure 30 Access to PEGS

7 MIGRATION ISSUES

The architecture described in the preceding sections covers a relatively static implementation of PEGS according to four different integration scenarios. Full care is given to the fact that the same PEGS may implement different integration scenarios between different Member States.

Starting from an empty page creates another level of complexity: how to synchronise information across Member States about which PEGS are available to which citizens and which businesses.

To reduce this additional complexity it is recommended to create on a Communal level a kind of PEGS catalogue service.

The PEGS catalogue service will contain a reference description of each PEGS to be considered for implementation. In addition it will describe for each Member State, or pair of Member States respectively, when this service will be available using what integration layer.

DOCUMENT CONTROL

Title: Architecture for pan-European eGovernment Services

Issue: Version 1.0

Date: 01/12/2004

Author: Johan Witters/Arnold van Overeem

Distribution: EC DG Enterprise – Bernhard Schnittger
Project Team

Reference: PEGS Infrastructure - Architecture

Filename: PEGS -Infrastructure Architecture v1.0.doc

Control: Reissue as complete document only

DOCUMENT SIGNOFF

Nature of Signoff	Person	Signature	Date	Role
Acceptance	Bernhard Schnittger			EC Project Officer

DOCUMENT CHANGE RECORD

Date	Version	Author	Change Details
01/10/2004	0.1	Johan Witters	Table of Content
11/11/2004	0.2 – 0.8	Arnold van Overeem	Initial draft and additions
12/11/2004	1.0	Johan Witters	Final review