PEPPOL Transport Infrastructure
Technical Overview
Statement of originality
This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Statement of copyright
This deliverable is released under the terms of the Creative Commons Licence accessed through the following link:
http://creativecommons.org/licenses/by/3.0/.

In short, it is free to
Share — to copy, distribute and transmit the work
Remix — to adapt the work

Under the following conditions
Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Author:
Carmen Ciciriello, SEPA International

Contributors:
Jens Jacob Andersen, Danish Agency for Digitization
Kenneth Bengtsson, Alfa1Lab

Published: November 2011
The purpose of this document is to provide interested organisations with a deeper understanding of the PEPPOL Transport Infrastructure, its key features, components and governance.

We assume the readers of this document have a general understanding of PEPPOL, its goals and the benefits of engaging in and promoting a fully automated, standards-based eProcurement environment.

For more information about the PEPPOL project, please see: http://www.peppol.eu
1. What is PEPPOL
1.1 Introduction
1.2 Building Blocks to Enable eProcurement

2. PEPPOL Transport Infrastructure
2.1 Introduction
2.2 Key Features
2.3 Key Components
2.4 Transport Interaction Scenario
2.5 PEPPOL Security Infrastructure

3. PEPPOL Governance Model

Annex 1: PEPPOL EIA repository and specifications
A structured approach to present the PEPPOL artifacts in a repository so that different stakeholders can access information relative to their specific needs, in a consistent and flexible way.

Annex 2: OSOR
PEPPOL provides many supporting software tools that are available on an open source licence from http://www.OSOR.eu

“The pan-European exchange of business documents between any private company and any EU governmental institution should be as easy as sending emails.”
Mikkel Leihardt
Head of Office, NITA
The Pan-European Public Procurement Online (PEPPOL) project was initiated in 2008 to provide standards-based IT infrastructure and services for cross-border public eProcurement in Europe.

While many European countries already use electronic procurement to make tendering of public sector contracts simpler and more efficient, most of these solutions are implemented solely on a national or regional level, with limited access to other communities.

The European Commission’s pilot project PEPPOL has not replaced, but instead built upon, the existing strengths of national eProcurement systems through agreement on specifications for cross-border procurement processes. By joining national eProcurement platforms and connecting eProcurement communities on a standardised backbone, companies can gain access to a vast public procurement market, resulting in increased opportunities for businesses, greater efficiencies and lower costs.

PEPPOL represents a major interoperability framework, covering the legal, organisational and technical perspectives.

This framework can create the foundation for the development of standardised software solutions for the complete eProcurement business cycle based on common documents and processes using an open exchange platform for electronic document transport across Europe.

What is PEPPOL?

The Pan-European Public Procurement Online (PEPPOL) project was initiated in 2008 to provide standards-based IT infrastructure and services for cross-border public eProcurement in Europe.

The PEPPOL project has developed standard specifications for content and business processes, and in 2010, established and tested an open exchange infrastructure across Europe.

From spring 2011, the PEPPOL project started its production pilot phase with organisations using PEPPOL solutions, including eAttestations in Virtual Company Dossiers used in a national post-award context, and the exchange of cross-border electronic invoices within the Nordic region and in Italy. Additionally, the PEPPOL eSignature validation service enables contracting authorities to validate qualified eSignatures from any European country.

Following the completion of the project, it is expected that the PEPPOL community will continue to exist and evolve through a combination of public and private sector adoption, based on PEPPOL guidelines and the continued operations of centralised components.

The PEPPOL consortium is comprised of leading public eProcurement agencies in 11 countries: Austria, Denmark, Finland, France, Germany, Greece, Italy, Norway, Portugal, Sweden and the United Kingdom. PEPPOL activities are funded jointly by individual Member States and the European Commission.
Building Blocks to Enable eProcurement

PEPPOL’s success is based on a modular building block approach, where organisations can grow their PEPPOL usage together with their expanding capabilities in eProcurement.

For the pre-award phase, PEPPOL includes the following sets of solutions to support the public tender process:

- Validation of eSignatures issued by certificate authorities
- Virtual Company Dossier to request and submit standardised company information and mutually recognised evidence (candidate statements, certificates and attestations)
- eCatalogue to request and submit standardised and formatted information (mainly used by Contracting Authorities to define and structure their request for goods and services using standardised properties and classifications provided by the PEPPOL Properties Server).
- A Transport Infrastructure available for the pre-award processes but used mainly in the post-award phase.

For the post-award process, PEPPOL includes:

- eCatalogue to exchange information about goods and services available under the contract
- eOrdering and eInvoicing using a defined set of processes to share common business information
- Validation of eSignatures issued by certificate authorities
- A Transport Infrastructure

The data models for the documents use common structures and reusable components. This makes it possible to build an order document with information from a catalogue and to create an invoice document from an order without retyping information, thereby reducing the manual work required and limiting the risk of errors in the procurement phase.

PEPPOL’s transport infrastructure interconnects eProcurement systems using common and nationally compatible standards. Access to the PEPPOL infrastructure takes place through Access Points, which are currently provided by both government agencies and private companies. By defining profiles and tools for interoperability on both a national and international scale, PEPPOL seeks to join the islands of eProcurement that currently operate across Europe.

Once connected to the PEPPOL Transport Infrastructure, organisations can reach any other community already using the PEPPOL network.
Public agencies and private enterprises can use the PEPPOL infrastructure to send and receive electronic documents by connecting to the Access Points, which are the base elements of the infrastructure.

PEPPOL Access Points (APs) form a secure network by connecting to each other using the same transport protocol and document format, applying digital signature algorithms to secure message content. Operators of APs connect to their customers through existing networks and use the PEPPOL network to exchange documents with each other. The figure below shows the main components of the PEPPOL transport infrastructure:

In order to route the documents received from the sender to the correct recipient, the Access Points in the network need to discover each other. The PEPPOL infrastructure maintains centralised addressing and metadata information on servers called Service Metadata Publishers (SMPs), which contain the addresses of the parties’ Access Points.

SMPs store information about the users connected to the PEPPOL network (receiving capabilities), providing details about the business document types supported and the business collaboration profiles that can be processed through the national infrastructure. The final key entity in the infrastructure is the Service Metadata Locator (SML).

The sender of an electronic document (for example an eInvoice, an eOrder or an eCatalogue), which can be a large corporation, an SME or a public administration, uses an Access Point to connect to the PEPPOL network, specifying the type of document being sent and the recipient, uniquely identified in the network by a business ID. Access Points can either be built by organisations or sourced as a service from IT providers offering PEPPOL capabilities.

Whether a sender or a recipient, every participant in the PEPPOL network is registered in an SMP, and the Access Points must know which one to connect to in order to retrieve the metadata about that specific recipient party. The SML contains the related SMP for every business ID.
Key Features

BusDox, a Common Electronic Document Exchange Platform

The PEPPOL transport infrastructure uses a set of technical specifications known as BusDox (Business Document Exchange Network) to allow organisations to securely and reliably exchange electronic documents. BusDox is document agnostic, meaning users can transfer ANY type of XML document between ANY network. In PEPPOL’s first pilot phase, a specific suite of business documents was developed, establishing a solid foundation to exchange additional document types in the future.

PEPPOL Access Points communicate to each other using the BusDox messaging system, a standardised and trusted way to exchange documents. BusDox also provides a pan-European addressing mechanism for eBusiness participants, making it easy to look up participants and to publish eBusiness capabilities.

By creating a transport infrastructure based on BusDox, PEPPOL makes it possible for any public or private European organisation to exchange electronic documents. This is reminiscent of the way governments established the road and railway infrastructure that enabled cross-border trade.

The BusDox specifications are based on a combination of W3C and OASIS standards, and are being maintained by an OASIS Technical Committee.

Open 4-Corner Model

An important difference between the BusDox standards and other messaging solutions is that BusDox is designed to support what is known as a 4-corner model where communication takes place between two Access Points, respectively for the sender and the recipient organisation.

Each Access Point derives the endpoint addresses of other Access Points through the BusDox SMP Infrastructure. Access Points may communicate via optional BusDox Transport Profiles, but they must always offer a START (Secure Trusted Asynchronous Reliable Transport) endpoint with which any other Access Point may communicate.

An important advantage of the open 4-corner model that PEPPOL employs is that any interested participant can access the network through a PEPPOL Access Point provider. However, any company in Europe (e.g.: contracting authority, economic operator) may set up an Access Point, providing it meets the PEPPOL requirements.

Addressing Independent of Transport

PEPPOL designed the Universal Endpoint addressing scheme (UPIS) to allow any type of existing addressing scheme to be mapped onto the PEPPOL scheme. PEPPOL uses a set of predefined document and process identifiers.

Participant identifiers of different schemes are supported (e.g. DUNS, GLN), while existing identifiers are re-used and assembled in a specified way. In PEPPOL, the participant identifier uses a combination of a reference to an issuing agency and a unique identifier issued by that agency. Identifiers may have different values, but the method by which they are defined is consistent.
Service Metadata Publisher (SMP)
The SMP contains the receiving capabilities of the Transport Service (Access Point) as a combination of Process, Document, the exact location (IP address) of the Transport Service (Access Point) according to receiving capabilities, and the REST API for interaction (pure HTTP). It makes it possible to dynamically explore and match capabilities online.

The PEPPOL infrastructure assumes that there are several SMPs in the infrastructure. There may even be several SMPs within a national domain. Thus, there is a need for specific agreements to ensure that the SMP Provider adequately provides the required services and that they have the required access to the Service Metadata Locator (SML).

Service Metadata Locator (SML)
The Service Metadata Locator is the key component that enables the pan-European eBusiness register for the exchange of business documents. The SML defines the profiles for the discovery and management of interfaces for the BusDox Service Metadata Locator service.

The Service Metadata Locator service specification is based on the use of DNS (Domain Name System) lookups to find the address of the Service Metadata for a given participant ID. This approach does not need a single, central server to run the discovery interface (with its associated single point of failure). Instead, the already distributed and highly redundant infrastructure that supports DNS is used. The SML service itself provides controlled access to the creation and updating of entries in the DNS.

For a sender, the first step in the discovery process is to establish the location of the Service Metadata relating to the particular Participant Identifier to which the sender wants to transmit a message. Each participant identifier is registered with only one Service Metadata Publisher. The sender looks up the endpoint for the Service Metadata Publisher using the DNS-based Service Metadata Locator service (this is a regular DNS resolve). The sender can then retrieve Service Metadata using Service Metadata Publisher services to obtain the metadata about the Participant Identifier, which includes the information necessary to transmit the message to the recipient endpoint represented by that Participant Identifier.

The SML management interface is the only centralised component in PEPPOL. At runtime, the SML uses decentralised DNS for load balancing of runtime requests, thus supporting a full European-wide upscaling of runtime performance.

START Profile
The START (Secure Trusted Asynchronous Reliable Transport) profile is the full profile that includes all the security and reliability features provided by the infrastructure. It is used for communicating between two Access Points.

START is based on Web-Service technologies, and it employs several WS-standards, including:

- WS-Addressing 1.0 to address remote resources (APs, SMP/SML)
- WS-Transfer, as a standard approach to accessing the message channels
- WS-Reliability, to ensure reliability of message exchange
- WS-Security 1.1 to manage authentication, autorisation and signatures on exchanged messages
- SOAP 1.1
- SAML 2.0

SAML 2.0 security tokens are used to carry security information across the infrastructure. SAML 2.0 protocol is based upon assertions, which carry the security claims (keys, certificates, references to external authorities) and the conditions under which the information is valid. A compliant implementa-
tion of a PEPPOL AP must be able to support the START profile.

The LIME Profile
The Lightweight Message Exchange Profile (LIME) protocol is a simple mechanism that allows an application to deliver a message to the Access Point to which it subscribes. The LIME Profile is designed to allow systems to participate in the BusDox infrastructure without needing to access service metadata or host an Access Point. Instead, they rely on an Access Point operator to provide Lightweight Message Exchange Profile (LIME) services to them. The LIME protocol alone does not enable the application to access the PEPPOL infrastructure, as all communications between access points use the START protocol.

A simple analogy is Internet email; large companies may run their own Simple Mail Transport Protocol (SMTP) server and proprietary email clients to create and read messages, but individuals or small companies rely on an ISP to provide an SMTP Relay and POP3 or IMAP server.

Key features of LIME include:
• No requirement to host online endpoints
• No firewall crossing
• No server infrastructure
• No requirement to support “advanced” WS-standards, such as WS-Trust, WS-Reliable Messaging
• Only minimal requirement to support WS-Security (authentication headers only)

A LIME AP may be an existing VAN or a new service offered by governments or private companies.

PEPPOL Identifiers
The PEPPOL transport infrastructure uses a set of identifiers to address resources and to define them uniquely:
• Participant Identifier identifies a sender/receiver on the PEPPOL network (standard schemes such as GLN, DUNS, CVR can be used)
• Document Identifier identifies a document type in the PEPPOL network
• Process Identifier identifies the process in which the document can participate
• Message Identifier identifies the single message across multiple hops in the network

The participant identifier uses a combination of reference to an issuing agency and a unique identifier issued by that agency. The use of an identifier issued by any of the issuing agency schemes is mandatory.

For example, the issuing agency for Danish company numbers has the identifier 9902 in PEPPOL. Company A is a Danish company with the unique Danish company number (in Denmark called CVR number) DK28158000. Therefore, Company A’s PEPPOL participant identifier is 9902:DK28158000.

For document and process types and schemas, PEPPOL supports (and encourages) the use of UBL 2.0 documents and CEN/BII profiles. A PEPPOL Business Interoperability Specification (BIS) is a CEN BII Profile with additional legal, organizational and technical requirements to support pan-European use.

The above information is carried along in the header of the SOAP messages defined by START and LIME profiles. SMPs use the identifiers to return to the requesting AP the address of the recipient AP. APs have to submit the recipient business identifier, the document identifier and the process identifier in their queries to the SMP.

The use of identifiers in PEPPOL is specified in the ‘Policy for Using Identifiers’.

For more information please see:
How do I transport the document?
Company B (a supplier) wants to send an invoice to Company C (a contracting authority/buyer) through the PEPPOL transport infrastructure. Please note that, in the diagram below, an Operator can be any Contracting Authority or Economic Operator who develops an Access Point for its own use. A service provider can set up an Access Point for commercial use.

Figures 4: Transport interactions

1. Operator 1 (used by Company B) connects to a PEPPOL Access Point in its country (AP1)

2. AP1 sends the business ID of the receiver (Company C) to the DNS system - Service Metadata Locator (SML)

3. The DNS system (SML) returns the address of Company C’s Service Metadata Publisher (SMP) registry

4. AP1 queries the SMP for the Company C AP address, submitting the business ID of the receiver, the document type and the process type

5. SMP returns the address of the PEPPOL AP1

6. AP1 sends the message containing the document to AP2

7. AP2 forwards the message to Operator 2 in country B

8. Operator 2 processes the document and sends it to Company C

Please see: http://www.peppol.eu/peppol_components/peppol-eia/ict-architecture/transport-infrastructure/framework
The PEPPOL Security Infrastructure rests on five pillars:

1. Trust is established using a Public Key Infrastructure (PKI)

2. Service providers sign an agreement before they join the infrastructure
   - Agreement regulates responsibilities, requirements, liability
   - Compliance checks may be performed

3. Secure communication protocols
   - Employs encryption, signing, certificates, security tokens

4. Operational security requirements for service providers
   - Firewalls, intrusion detection, patching, logging, penetration test

5. Sender authentication
   - Sender Access Point vouches for sender identity

Security Scope

Infrastructure security scope:
- Communication to/from AP / SMP / SML (i.e. not end-to-end)
- Independent of payload
- Sender authentication

Outside of scope:
- Document or business level security:
  - Between sender and receiver (end-to-end)
  - Requirements for payload (e.g. signed and/or encrypted documents)

Existing Infrastructure Sphere

Infrastrucrure security scope:
- Communication to/from AP / SMP / SML (i.e. not end-to-end)
- Independent of payload
- Sender authentication

Out of scope:
- Document or business level security:
  - Between sender and receiver (end-to-end)
  - Requirements for payload (e.g. signed and/or encrypted documents)

Figure 5: PEPPOL Security Infrastructure Scope
PEPPOL Security Infrastructure

PEPPOL Root PKI
The PEPPOL ROOT PKI is used to create the core circle of trust in PEPPOL between APs, SMPs and SML. Together with the use of SAML Sender Vouchers assertion tokens, this creates a flexible and trustworthy 4-corner model for realising the foundation of pan-European document exchange.

A PKI can be established by:
1. A Certificate Authority (CA) issuing digital certificates under a central PEPPOL root certificate
2. Anyone with a PEPPOL certificate - considered a valid member of the infrastructure (closed user group PKI)
3. The PEPPOL Governing Board acts as Registration Authority

Advantages:
• The CA service can be acquired as a standard offering by PKI vendors
• Service providers can validate peers just by installing the PEPPOL root certificate (does not need to invoke services)
• Validation of certificates is offered out-of-the-box in most middleware
• Proven technology and scalable
• Easy to revoke members
• Reasonable cost (centralised)

Figure 6: PEPPOL “Circle of Trust”
PEPPOL Security Infrastructure

Linking Trust and Agreements

Service Providers can only join the infrastructure (and receive a PEPPOL certificate) once they have signed the relevant agreements with the PEPPOL Governing Board. When entering the agreement, service providers commit to fulfil the stated quality and security requirements. The PEPPOL Governing Board may perform checks on new Service Providers, including a review of documentation and a review of auditor statements on compliance.

Secure communication is achieved by:
1. Signing SOAP messages (WS-Security)
   • Authentication of service providers
   • Message integrity
2. Using transport-layer security (SSL / TLS)
   • Confidentiality & integrity
3. Including SAML tokens vouching for sender identity (WS-Security)
   • Sender authentication
4. Similar to OIO Identity-Based Web Services

Sender Authentication
A Sender Access Point is required to authenticate the sender of document and vouch for its identity to the recipient. This relieves the Recipient from the complexity of handling many different types of credentials, and means that the Recipient needs only to know sender identity, not the details of its credential.

Key Features
1. Sender Access Point issues SAML 2.0 token stating:
   • Sender identity (result of authentication)
2. Level of identity assurance (1-4)
3. Issuer of token (signed with PEPPOL certificate)
2. Level of identity assurance:
   • 1=> low confidence in claimed identity
   • 4=>very high confidence in claimed identity
3. Technology agnostic
4. Assurance level classified according to Liberty Alliance Identity Assurance Framework, taking into account:
   • Technical quality of the credential
   • Credential issuing process
   • Organizational factors

![Figure 7: PEPPOL authentication](image-url)
PEPPOL Governance Model

The long term governance model for the PEPPOL Transport Infrastructure is built around two levels of authority.

1. European-wide coordination, which is achieved through centralised governance of the PEPPOL SML and the common technical standards and specifications.

2. National and/or regional coordination, which is achieved by delegating governance over the implementation and use of PEPPOL SMPs and PEPPOL APs to an appointed PEPPOL Regional Authority.

**European Coordination**
European-wide coordination is achieved through the PEPPOL Coordinating Authority, which has authority over all central components of the PEPPOL Transport Infrastructure. Key aspects of this responsibility include:

- Manage updates and releases of new versions of PEPPOL technical standards and service specifications according to the published policy
- Central governance of the PEPPOL Public Key Infrastructure (PKI) according to the published policy, including the authority to issue digital certificates, as well as suspend and revoke a digital certificate if a PEPPOL SMP Provider or PEPPOL AP Provider fails to fulfil its obligations
- Provide the PEPPOL SML service

Through these measures, a set of minimum requirements and criteria has been established and consistently applied throughout the full PEPPOL Transport Infrastructure.

Making the PEPPOL Coordinating Authority the instrument for managing areas of use (through the recognition of identification schemes) and using the PEPPOL SML as a tool to enforce this policy, consistency and interoperability will ensure support not only at technical level, but also on semantic and organisational level. Furthermore, the PEPPOL Coordinating Authority is responsible for:

- Providing a website to promote and provide support for the operation of the PEPPOL Transport Infrastructure, including tools to facilitate efficient sharing of information and contact between all actors involved in the infrastructure
- Providing an arbitration body for eventual conflicts related to any part of the PEPPOL Transport Infrastructure
- Appointing and signing the Community Agreements with relevant PEPPOL Regional Authorities
- Enter into agreements with and provide support for PEPPOL SMP Providers and PEPPOL AP Providers in domains where no PEPPOL Regional Authority has been delegated (e.g. in PEPPOL non-beneficiary countries)

**National and Regional Coordination**
The PEPPOL Regional Authority oversees the actual implementation and use of the PEPPOL Transport Infrastructure within a defined domain. The domain will typically be defined by national borders or by regions within a country. It is not foreseen that domains will overlap or cross national borders.

Key aspects of the responsibility of the PEPPOL Regional Authority include:
PEPPOL Governance Model

- Describe and make publicly available any additional qualification criteria applicable to PEPPOL SMP Providers and PEPPOL AP Providers with whom they will contract - such additional qualification criteria typically include service requirements over and above what is defined by the PEPPOL Coordinating Authority.
- Sign agreements with the qualifying PEPPOL SMP Providers and PEPPOL AP Providers.
- Governance of the PEPPOL Public Key Infrastructure (PKI) by participating in the processes required to issue digital certificates, as well as suspend and revoke a digital certificate if a PEPPOL SMP Provider or PEPPOL AP Provider fails to fulfill its obligations.
- Ensure that PEPPOL SMPs and PEPPOL APs established within its domain comply with the minimum requirements defined by the PEPPOL Coordinating Authority, as well as with any additional qualification criteria applicable within the domain.
- Provide support for PEPPOL SMP Providers and PEPPOL AP Providers contracting with the PEPPOL Regional Authority, including the escalation of support issues that the PEPPOL Regional Authority cannot resolve to the PEPPOL Coordinating Authority.

For European countries or regions that have not nominated a PEPPOL Regional Authority or do not wish to establish any specific national governance, including qualification requirements for PEPPOL SMP Providers or PEPPOL AP Providers, the governance model and qualification requirements established by the PEPPOL Coordinating Authority will apply.

PEPPOL Agreements
The figure below illustrates the operational components of the PEPPOL Transport Infrastructure, the actors involved in their operation and the agreements required.

![Figure 8: PEPPOL Governance Model](image-url)
The PEPPOL Transport Infrastructure Agreements (TIA) include three types of agreements:

1. PEPPOL Community Agreement
2. PEPPOL Access Point (AP) Provider Agreement
3. PEPPOL Service Metadata Publisher (SMP) Provider Agreement

The regime of agreements and the governance structure ensure that:

- the role and responsibilities of each actor are clearly described and openly available, making PEPPOL an open and transparent community
- sufficient information is made available through the SML/SMP, allowing a Participant to make this its sole source of information for conducting eProcurement with its trading partners

It should be noted that the Business Agreement, as well as the Participant Agreement, shown in the above figure are not part of the PEPPOL Governance models. It is, however, expected that such agreements may include provisions related to the use of the PEPPOL Transport Infrastructure.

**Structure of the PEPPOL Agreements**

The PEPPOL Community Agreement is provided as a set agreement with identical provisions applicable to all PEPPOL Regional Authorities to ensure common governance for the full PEPPOL Transport Infrastructure.

The PEPPOL AP Provider Agreement and the PEPPOL SMP Provider Agreement are provided as “template documents” allowing each Regional Authority to adjust the actual text and language of the agreements, according to local terms and conditions, including alignment to local legislation. To ensure interoperability and consistency across domains, the “template documents” identifies provisions that must be present in any PEPPOL AP Provider Agreement and PEPPOL SMP Provider Agreement.

All three types of agreements share a common set of annexes defining technical aspects related to the services. By making these annexes commonly applicable for all agreements a set of minimum requirements and criteria are established and consistently applied throughout the full PEPPOL Transport Infrastructure.

The PEPPOL Agreements and the seven Annexes are available at the following link:

http://www.peppol.eu/peppol-components/peppol-eia/governance/transport-infrastructure/models

For contact details and more information about the PEPPOL Coordinating Authority, please see:

http://www.peppol.eu/peppol_components/-transport-infrastructure/governance/peppol-coordinating-authority

For contact details and more information about the PEPPOL Regional Authorities, please see:

http://www.peppol.eu/peppol_components/-transport-infrastructure/governance/peppol-regional-authorities
ANNEX 1

PEPPOL EIA repository and specifications

The PEPPOL Enterprise Interoperability Architecture (EIA) is a structured approach to present the PEPPOL artifacts (project documents, specifications, user guides, software tools, etc.) in a repository so that different stakeholders can access information relative to their specific needs, in a consistent and flexible way.

The EIA repository presented below as three dimensional matrix is a useful tool for organisations interested in implementing the PEPPOL components, and become familiar with the results of the project.

The EIA consists of 4 main Components (defined as “Communities”):

- eSignature Validation Infrastructure – validates eSignature certificates across EU borders.
- Transport Infrastructure – enables pan-European eDelivery of business documents between the eProcurement communities
- Post-Award eProcurement - enables the purchasing process consisting of eCatalogue, eOrdering and eInvoicing
- Pre-Award eProcurement - enables the tendering process currently consisting of eAttestation (VCD) and eCatalogue

Where each Component has 6 dimensions:

- ICT Architecture – providing the ICT scope, solutions and ICT architecture for the interoperability community.
- Conformance and Test – comprising the requirements, processes and tools of conformance for the different interoperability stakeholders.
- Life Cycle Management (LCM) – processes for LCM of business and ICT architectures.
- Governance - comprising the governance structure, legal framework and processes for the business and ICT architectures.
- Marketing – including processes and material for increasing awareness and recruiting new participants for PEPPOL pilot projects.
- Business – being the business scope and business architecture of the interoperability community.

And 6 layers (defined as “Abstraction levels”)

- Strategy
- Framework
- Models (guidelines and specifications of the different services and components)
- Services and Components
- Designs
- Implementations

For more information please see:
http://www.peppol.eu/peppol_components/peppol-eia

The PEPPOL EIA repository includes the BusDox specifications:
The link above provides the following documents:

- Common Definitions
- Service Metadata Publishing
- Service Metadata Locator Profile
- Secure Trusted Asynchronous Reliable Transport
- Lightweight Message Exchange Profile
- PEPPOL Identifier Schemes

and the PEPPOL Sample software:

http://www.peppol.eu/peppol_components/peppol-eia/ict-architecture/transport-infrastructure/services-components

ANNEX 2
Open Source Observatory and Repository (OSOR)

PEPPOL provides many supporting software tools that are available on an open source licence from www.OSOR.eu (the Open Source Observatory and Repository for European public administrations).

Joining the PEPPOL OSOR community also provides access to a collaborative forum for software developers.

For more information please see:
http://www.osor.eu