PEPPOL
PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE

eSignature Infrastructure Marketing Model

eSignature Long Demo

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Objectives of PEPPOL eSignature

The overall objective of PEPPOL eSignature is to provide cross European interoperability of electronic signatures, focussing on the verification process.

3 steps to reach that goal:

- Definition of a trust model for validation services federation.
- Specify the way of signing eProcurement data and validating them.
- Provision of solutions for verification of signatures.

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Signatures and certificates: Validation vs. Acceptance

Signature and certificate validation (cryptography, technical), Signatures must be valid

- Computationally correct and valid eID used

Signature and certificate acceptance, Signature must be acceptable by the Contracting Authority

- Acceptance criteria: Legal/regulatory requirements and/or risk assessment
  - Certificate quality sufficient?
  - Approval status (national/international) of CA?
  - Cryptographic quality sufficient?
  - Not possible to assess using only “traditional PKI” elements

⇒ Signature policies to define acceptance criteria – quality being the main issue

⇒ “Rich validation interfaces” to assess policy fulfilment

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

PEPPOL eSignature

PEPPOL does not help you to sign

- Signing in a web user interface using “any” smart card or other signature solution is yet to be solved
- PEPPOL assumes that actors (notably economic operators) are able to sign locally using their preferred, national eID solution

PEPPOL helps you verify and accept signatures

- An economic operator from any Member State uploads signed documents for a tender
- PEPPOL validation service enables verification of signatures regardless of originating country (inside EU/EEA and to some extent outside)
- Verification also of eID quality and national approval status in originating country (status must be recognised cross-border)

PEPPOL may help you specify conditions for signatures

- Signature policy framework to set requirements

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Infrastructure Components

1.) PEPPOL XKMS Responder

- The PEPPOL XKMS Responder can validate certificates against configured CAs.
- It can use the PPRS to pass XKMS request towards other PEPPOL XKMS responders.

2.) PEPPOL Public Registry Service (PPRS)

- The PPRS is a service that provides information about Validation Service Providers.
- The PPRS is organised according to Trust-service Status List (TSL, ETSI TS 102 231)

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

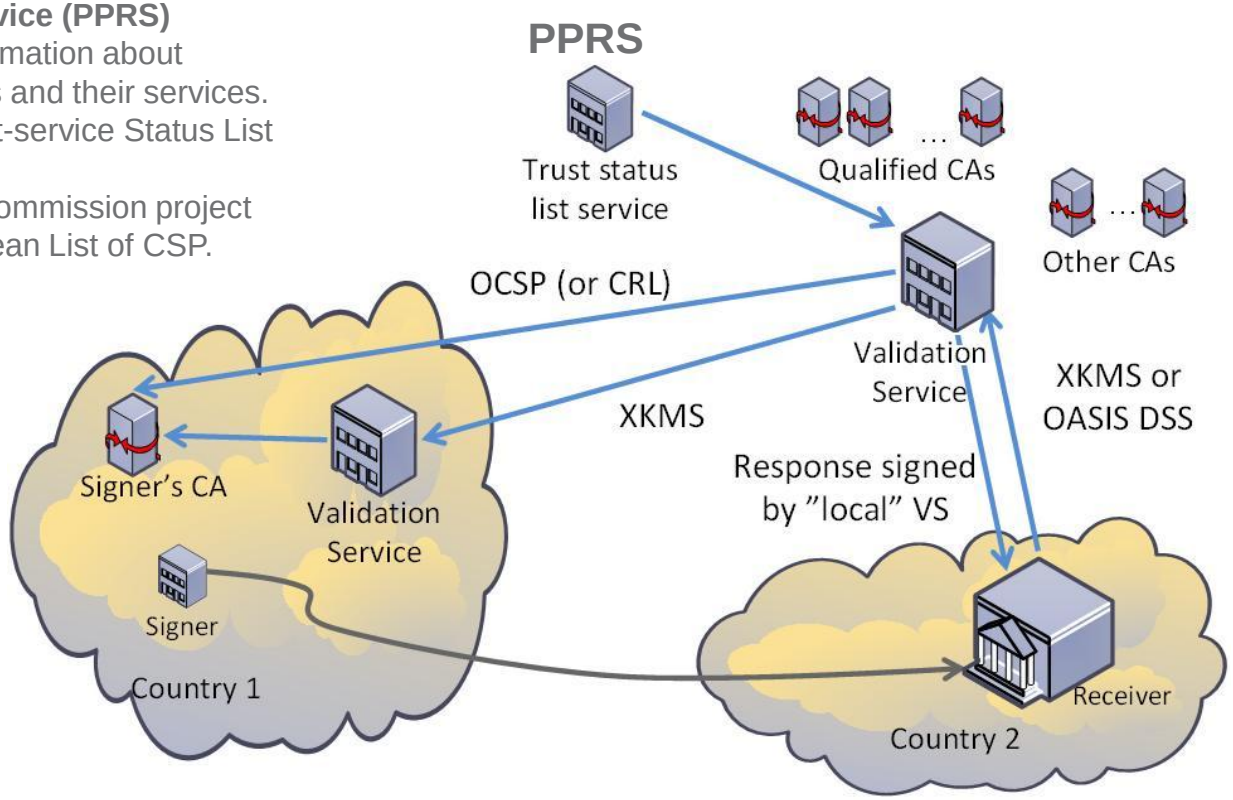
Overall concept of WP1-solution

Infrastructure Components for trans-national eSignature Certificate Validation

1.) PEPPOL XKMS Responder: can validate certificates against configured CAs and use the PPRS to pass XKMS request towards other PEPPOL XKMS responders.

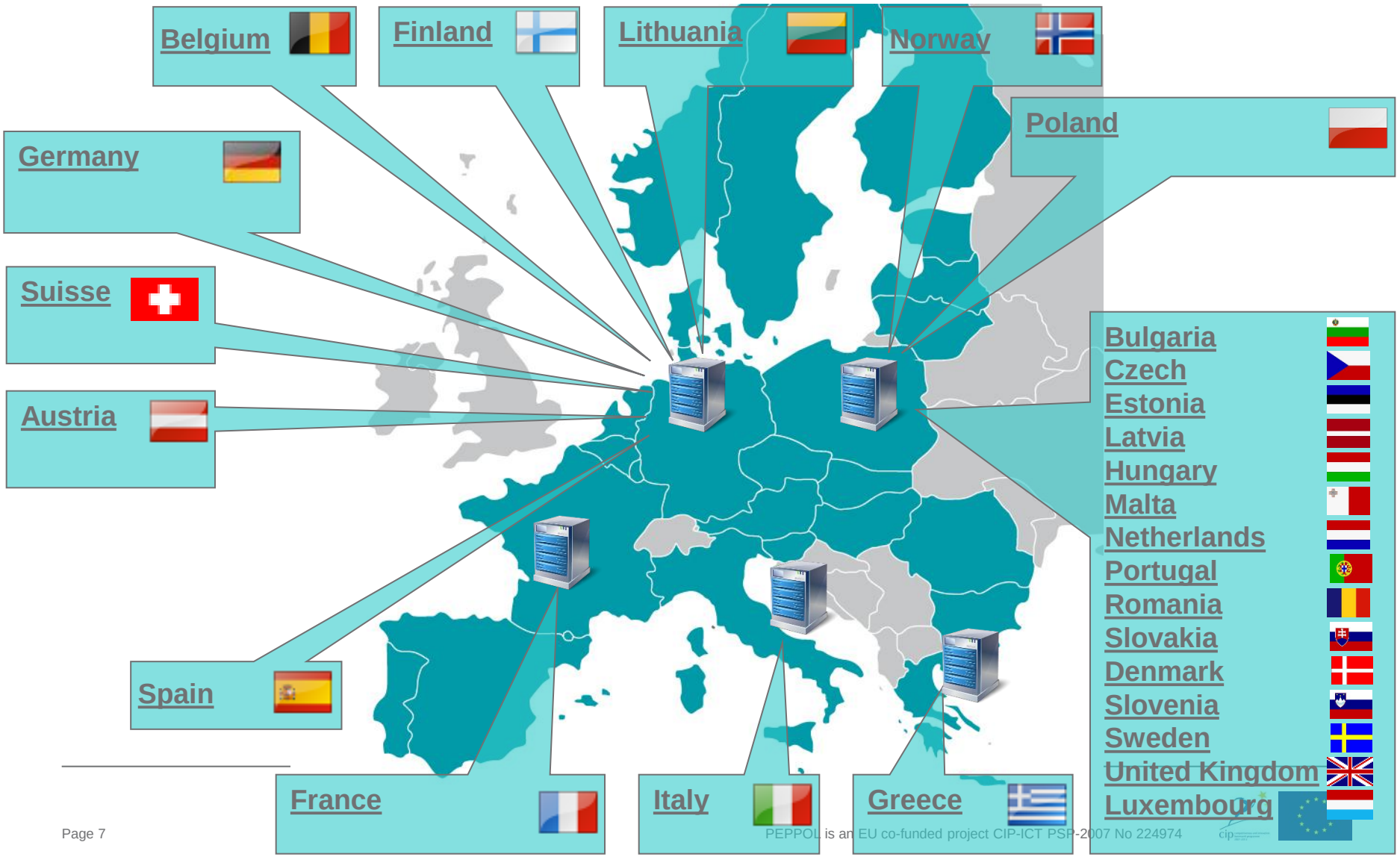
2.) PEPPOL Public Registry Service (PPRS)

- Service that provides information about Trusted Service Providers and their services.
- Organised according Trust-service Status List (TSL, ETSI TS 102 231)
- It is aligned with the EU Commission project on establishing an European List of CSP.



PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

All CAs from EU-TSL



PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

The Validation Service System

Chained, national validation services

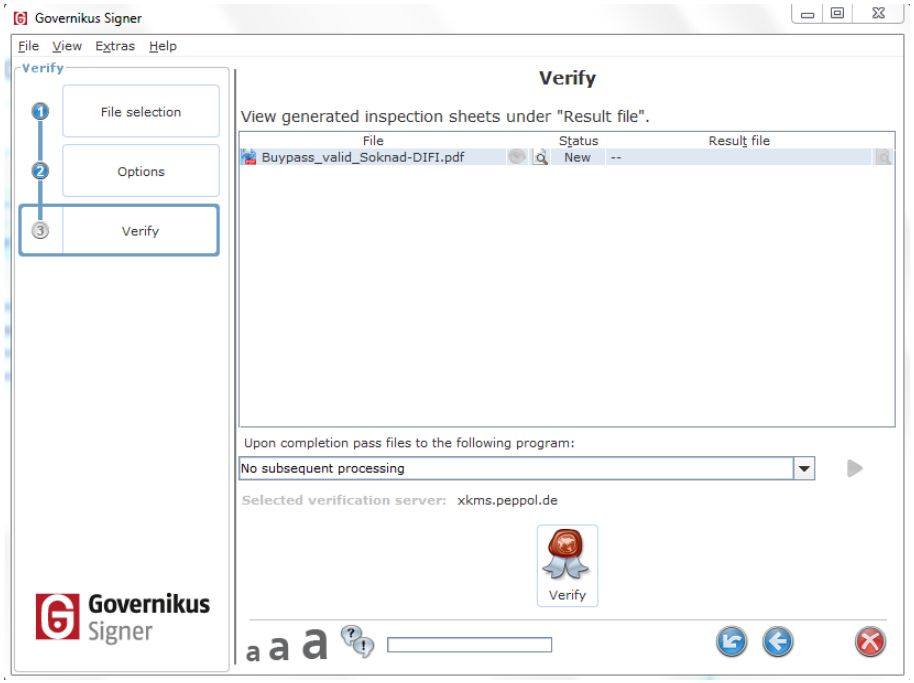
- Established for Germany, France, Italy, Greece
- National coverage plus more
- National approach may be required in some countries

“International” validation service

- Established for PEPPOL by Norway
- Agreement with Unizeto (Poland) – Web Notarius service
- Covers as broad as possible on its own
- May use the national validation services
- Current coverage about 300 eID issuers in EU/EEA plus Russia, Ukraine etc.

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Validation with Stand Alone Client



Norwegian Signature

Inspection sheet from 2011-10-23 19:32:24

Structure

PDF document: Buypass_valid_Soknad-DIFI.pdf

PDF revision: Signature2

Author JON BJØRGE ØLNES All applied verifications are positive.

Signature checks

Signature check PDF revision Signature2

Author	JON BJØRGE ØLNES
Issuer of certificate	Buypass AS-983163327
Signature level	Advanced signature with qualified certificate (EU)
Signing time	2009-01-09 11:02:24
Inspection time	2011-10-23 19:32:18

Content signature check

	Hash	Signature
Cryptographic content signature check		
Used algorithms	SHA1	RSA-1023

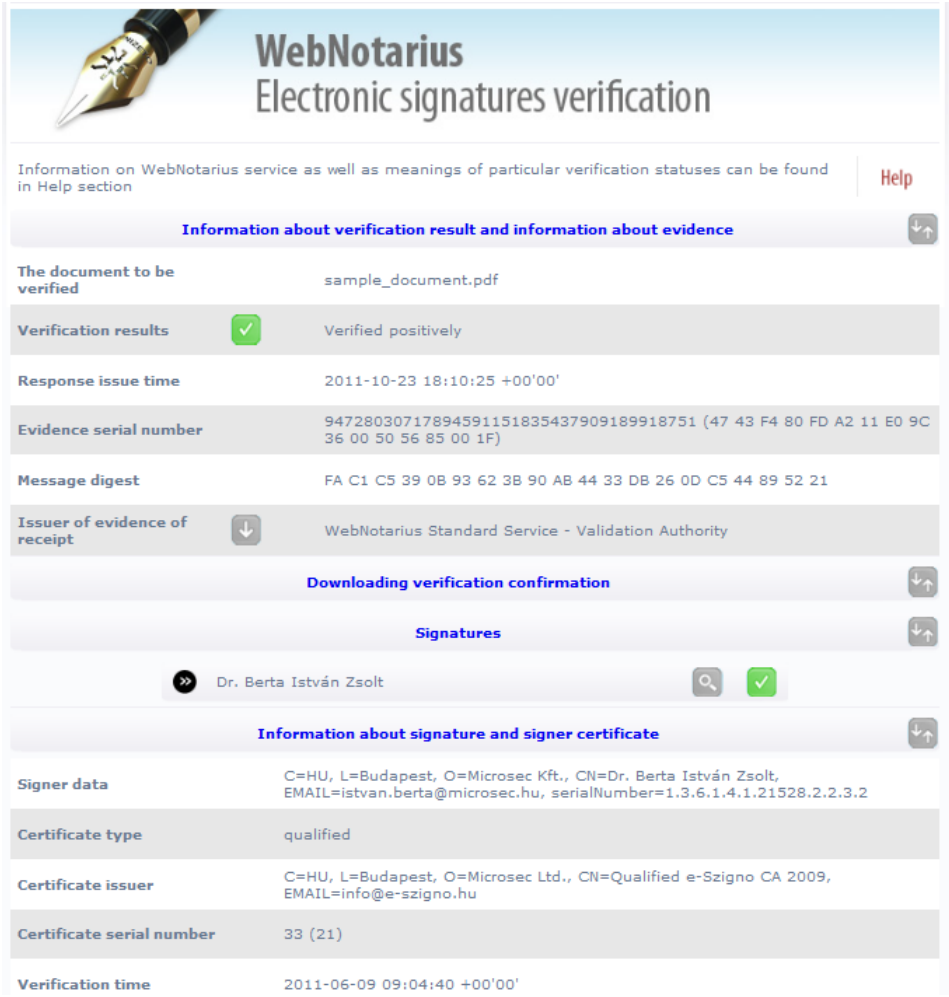
Signature certificate check

	Hash	Signature
Issuer trust		
Cryptographic certificate chain signature verification		
Certificate validity interval		
Revocation state (not revoked)		
Used algorithms	SHA1	RSA-2048

Technical information

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Validation on Web Portal



WebNotarius
Electronic signatures verification

Information on WebNotarius service as well as meanings of particular verification statuses can be found in Help section

Help

Information about verification result and information about evidence

The document to be verified	sample_document.pdf
Verification results	Verified positively
Response issue time	2011-10-23 18:10:25 +00'00'
Evidence serial number	947280307178945911518354379091899187 51 (47 43 F4 80 FD A2 11 E0 9C 36 00 50 56 85 00 1F)
Message digest	FA C1 C5 39 0B 93 62 3B 90 AB 44 33 DB 26 0D C5 44 89 52 21
Issuer of evidence of receipt	WebNotarius Standard Service - Validation Authority

Downloading verification confirmation

Signatures

Dr. Berta István Zsolt

Information about signature and signer certificate

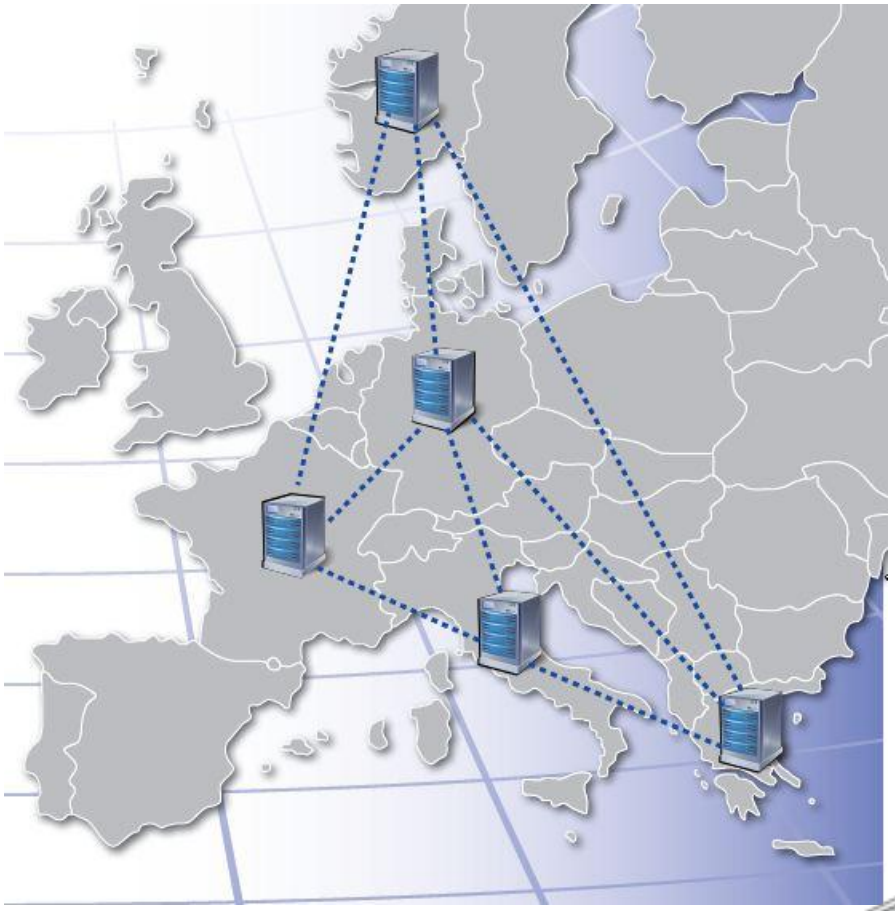
Signer data	C=HU, L=Budapest, O=Microsec Kft., CN=Dr. Berta István Zsolt, EMAIL=istvan.berta@microsec.hu, serialNumber=1.3.6.1.4.1.21528.2.2.3.2
Certificate type	qualified
Certificate issuer	C=HU, L=Budapest, O=Microsec Ltd., CN=Qualified e-Szigno CA 2009, EMAIL=info@e-szigno.hu
Certificate serial number	33 (21)
Verification time	2011-06-09 09:04:40 +00'00'

Hungarian Signature

https://standardva.webnotarius.eu/

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Infrastructure and Components ready to use



Open source server Software

Free to use validation client with API for integration

Own implementation towards XKMS interface (with Toolkit)

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Sustainability of the WP1 solution

- Will service providers offer PEPPOL eSignature solutions? **Yes**
  - Unizeto will continue to provide their validation service according to PEPPOL
  - bos integrates the XKMS-component in their product line Governikus
  - eprocurment providers AI, Mercell and EU-Supply integrates the WP1 solution in their product lines.
  - ADETEF, InfoCamere and the University of Piraeus will also continue their service.
  - Link for the French platform as example : https://www.marches-aube.fr/

- Will the PEPPOL specifications be maintained? **Yes**
  - PEPPOL WP1 team works with standardisation bodies OASIS / ETSI to bring the specifications to standardisation.

- ~~Will the Commission take over responsibility for central component? **Yes**~~
  - An operator for the PPRS will be chosen.

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Broader Impact at European Level

- Collaboration with SPOCS
  - SPOCS uses the PEPPOL validation infrastructure in its pilots.
  - PEPPOL eSignature and SPOCS are using the same governance model, based on the ETSI TSL specification.
- ETSI Technical Specification 102 231 (TSL) will incorporate in the next version the service type trusted validation service, motivated by PEPPOL eSignature expert group.
- Coordination with e-CODEX: e-CODEX states usability of solution and will use the WP1 eSignature infrastructure!
- WP1 provided and coordinated the PEPPOL input to the EC public consultation on eID and eSignatures.

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Summary and Outlook

- PEPPOL and particular the WP1 eSignature solution “is live”.
- Recruitment of PEPPOL users ongoing
  - E-procurement communities
  - Contracting Authorities & Buyer/supplier pairs
- PEPPOL enabled solutions and services about to be brought to market
- PEPPOL user community to involve private and public sector stakeholders in future governance to be established

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

Further Information

Up to date news, specifications, contact information:

www.peppol.eu

PEPPOL Enterprise Interoperability Architecture (EIA):

www.peppol.eu/peppol-eia

Open Source Observatory and Repository for European public administrations (OSOR) with the published components and community support:

http://www.osor.eu/projects/peppol/

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974

ePROCUREMENT WITHOUT BORDERS IN EUROPE

www.peppol.eu

PEPPOL is an EU co-funded project CIP-ICT PSP-2007 No 224974