



eSignature Infrastructure Marketing Model

eSignature Short Demo

Objectives of PEPPOL eSignature

▶▶ WHY does PEPPOL eSignature exist?

- ▶▶ To provide cross European interoperability of electronic signatures, focussing on the verification process.

▶▶ WHICH issues does it address?

- ▶▶ Signature validation service which can validate a high number of European digital signatures cross border.
- ▶▶ Quality classification of the digital signatures.

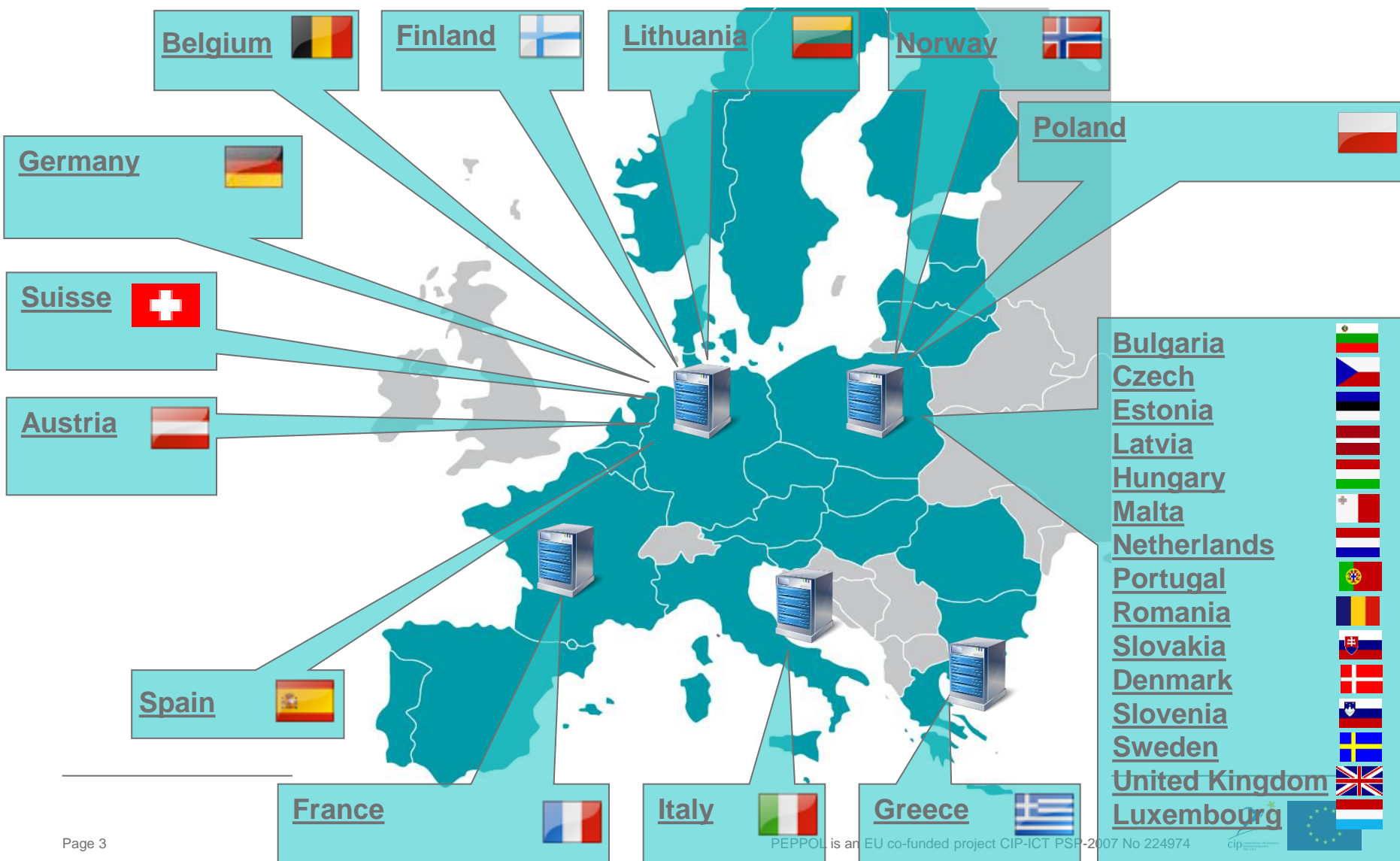
▶▶ WHAT are the benefits?

- ▶▶ High flexibility of solution: It can be implemented in any scenario with digital signatures.

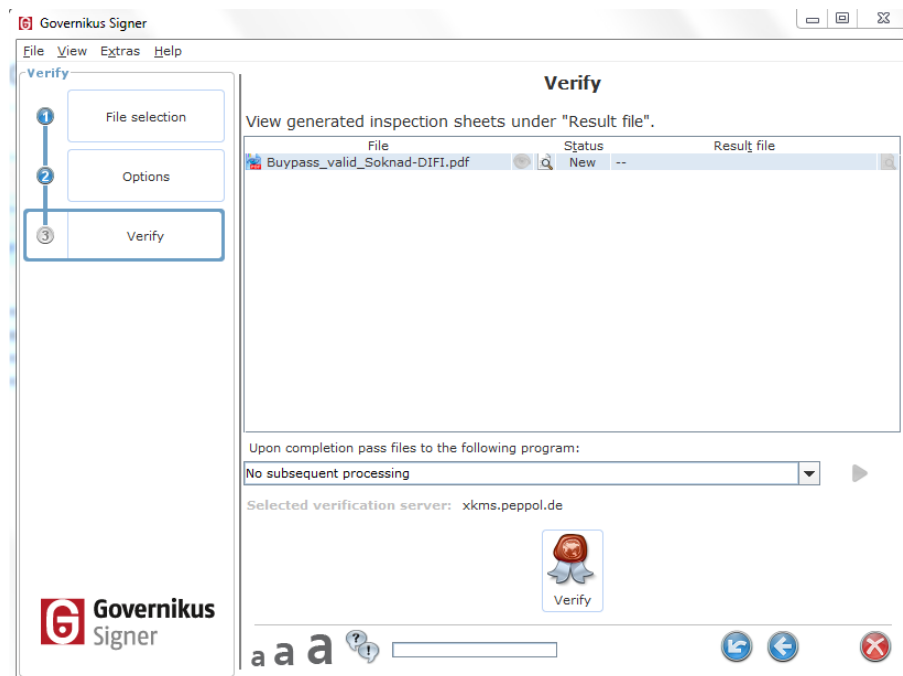
▶▶ WHO can benefit and HOW?

- ▶▶ Service providers can easily implement the solution and offer respective services and software.
- ▶▶ Contracting authorities can validate any digital signature.
- ▶▶ Economic operators can use their favoured signature solution.

All Qualified CAs from EU-TSL



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	<input checked="" type="checkbox"/> JON BJØRGE ØLNES All applied verifications are positive.

Signature checks

<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> Cryptographic content signature check	
<input type="checkbox"/> Used algorithms	
	Hash Signature
	SHA1 RSA-1023
Signature certificate check	
<input checked="" type="checkbox"/> Issuer trust	
<input checked="" type="checkbox"/> Cryptographic certificate chain signature verification	
<input checked="" type="checkbox"/> Certificate validity interval	
<input checked="" type="checkbox"/> Revocation state (not revoked)	
<input type="checkbox"/> Used algorithms	
	Hash Signature
	SHA1 RSA-2048
Technical information	

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	94728030717894591151835437909189918751 (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 38 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.bera@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/>

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)

eProcurement without borders in Europe

www.peppol.eu

