www.eu-spocs.eu

COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME
ICT Policy Support Programme (ICT PSP)

Preparing the implementation of the Services Directive

ICT PSP call identifier: ICT PSP-2008-2
ICT PSP main Theme identifier: CIP-ICT-PSP.2008.1.1

Project acronym: SPOCS

Project full title: Simple Procedures Online for Cross-border Services
Grant agreement no.: 238935

Specifications for interoperable access to eDelivery and eSafe systems

Appendix 2: Trust-service Status List profiling

("SPOCS-TSL")

- Corrigenda 1.1, February 2011 based on Version 1.0 -

Deliverable Id :	D3.2
Deliverable Name :	Specifications for interoperable access to eDelivery and eSafe systems
Status :	Corrigenda 1.1
Dissemination Level :	Public
Due date of deliverable :	30th September 2010
Actual submission date :	
Work Package :	WP3: Interoperable delivery, eSafe, secure and interoperable exchanges and acknowledgement of receipt
Organisation name of lead contractor for this deliverable :	**BVA**
Author(s):	Jörg Apitzsch (DE FHB), Luca Boldrin (IT InfoCert), Daniele Mongiello (IT InfoCert)
Partner(s) contributing :	SPOCS.AT, DE BVA, DE Siemens, GR MINT, IT InfoCamere, NL MINEZ, PL ILIM

Abstract: This document Appendix 2 is the second deliverable in work package 3 of the EU co-funded project SPOCS. It describes profilings and extension specifications for Trust-service Status List used by WP3 for trust establishment between different eDelievry and eSafe solutions to be interconnected. Based on the specifications open modules will be developed.

History

Version	*Date*	*Modification reason*	*Modified by*
0.9	31.8.10	Aligned and finalized; ready for QA	Luca Boldrin Jörg Apitzsch
0.9.1	15.9.10	Adjustment for eSafe	Luca Boldrin Bernd Martin
1.0	30.9.10	No modification regarding precedor submitted to and approved by EC	
1.1	11.2.11	Corrigenda according findings during first implementation phase	Jörg Apitzsch Daniele Mongiello Luca Boldrin

© SPOCS Consortium

Table of contents

List of tables

List of abbreviations

Abbreviation	Explanation
EC	European Commission
eID	Electronic Identity
MD	(eDelivery) Management Domain
MS	Member State
REM	Registered E-Mail
SPOCS	Simple Procedures Online for Cross-border Services
SSL	Secure Socket Layer
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trusted Service Provider
WP<n>	Work Package (number n)

Further abbreviations used in this document are explained on first occurrence.

© SPOCS Consortium

Document structure of SPOCS D3.2

SPOCS deliverable D3.2 "Specifications for interoperable access to eDelivery and eSafe systems" consists of several documents.

Main part gives a complete description of the general context, functionality of solutions provided, their architectural details and covered security and trust establishment features.

Additional documents are provided for detailed technical specifications of the buildings blocks, considered security architecture modelling and development baselines and according operational policies.

The main document:

- SPOCS D3.2 Functional Specification, Architecture and Trust Model

is accomplished by following separated appendix documents:

- Appendix 1: Security Architecture Development Process
- Appendix 2: Trust-service Status List Profiling ("SPOCS TSL")
- Appendix 3: eDelivery Interconnect Protocol and Gateway Specification
- Appendix 4: eSafe – Operations in Detail
- Appendix 5: SPOCS TSL Accreditation and Operation PolicyAppendix 6: Security Model.

This corrigenda is based on document Appendix 2: Trust-service Status List Profiling ("SPOCS TSL"), part of the second deliverable of SPOCS WP3.

Referenced XML Namespaces

Prefix	XML Namespace	Reference
rem	http://uri.etsi.org/02640/v1#	[12]
stsl	*Preliminary:* http://uri.eu-spocs.eu/tsl/v1#	This specification
tsl	http://uri.etsi.org/02231/v2#	[9]
sie	http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-TrustedList/#	[9]
xs	http://www.w3.org/2001/XMLSchema	[20]

Table 1: Referenced Namespaces

SPOCS TSL

The dominant role of the SPOCS TSL in the context of the WP3 concept is outlined in SPOCS D3.2 Functional Specification, Architecture and Trust Model, section 2.1, Trust model, while TSL operations is detailed there in section 2.2.4.

In the present document we define a profiling and additional extensions in order to serve SPOCS requirements.

The model is based on Trust-service Status List, as defined by ETSI TS 102 231 v3.1.2 [9], which admits for the incorporation of status information for general trusted services.

A different TSL conformant to the specifications will be set up for testing purposes. In order to avoid misuse its "Scheme operator name" will be set to "SPOCS - TEST" and it will be signed with a test certificate.

© SPOCS Consortium

1 TSL elements content profiling

Tag	Value	Required /Optional / NotUsed	Note
Trust-Service status List tag			
TSL Tag	According to TS 102 231	R	
Scheme information			
TSL version identifier	According to TS 102 231	R	The value of the identifier for TSL conforming to the version of TSL specifications.
TSL sequence number	TSL issue number	R	
TSL type	"**http://uri.etsi.org/TrstSvc/TSLType/generic**"	R	May change after project conclusion, depending on the adopted sustainability model. Might change to "**http://uri.etsi.org/TrstSvc/TSLType/schemes**" if a distributed TSL model will be chosen afterward
Scheme operator name	"SPOCS"	R	Will be changed after project conclusion, depending on the adopted sustainability model.
Scheme operator postal address	<SPOCS TSL maintainer postal address>	R	Will be changed after project conclusion, depending on the adopted sustainability model.
Scheme operator electronic address	<SPOCS TSL maintainer electronic address>	R	Will be changed after project conclusion, depending on the adopted sustainability model.
Scheme name	"SPOCS TSL"	R	Will be changed after project conclusion, depending on the adopted sustainability model.
Scheme information URI	<SPOCS TSL reference web page>	R	Will be changed after project conclusion, depending on the adopted sustainability model.
Status	"**http://uri.etsi.org**	R	It is not expected that

Tag	Value	Required /Optional / NotUsed	Note
determination approach	**/TrstSvc/TSLType/StatusDetn/passive**"		SPOCS will perform assessment of listed services. Will change to "http://uri.etsi.org/TrstSvc/TSLType/StatusDetn/list" if a distributed approach will be chosen afterward.
Scheme type/community /rules	"http://www.eu-spocs.eu"	R/ N	This field is required during the piloting phase. This field will not be used after project completion
Scheme territory	"EU"	R	
TSL policy/legal notice	<text - as a multilingual character string >	R/N	Text specifying piloting conditions under which the SPOCS TSL is deployed. This field will not be used after project completion
Historical information period	0	R	No historical information will be maintained in the piloting phase. Will remain "0" if the distributed model will be chosen afterwards.
Pointers to other TSLs	--	N/O	Not used in piloting phase. Will be used if distributed model will be chosen afterwards.
Additional information field	--	N/O	Not used in piloting phase. May be used if distributed model will be chosen afterwards.
List issue date and time	According to TS 102 231	R	UTC at which the TSL was issued
Next update	According to TS 102 231	R	latest date and time by which the next planned update of the TSL will be made available
Distribution points	**"http://www.eu-spocs.eu/TSL/currentTSL"**	R	Will be changed after project conclusion, depending on the adopted sustainability model.

Tag	Value	Required /Optional / NotUsed	Note
Scheme extensions	--	N	Not envisaged
TSP Information			
TSP name	According to TS 102 231	R	
TSP trade name	According to TS 102 231	O	
TSP address	According to TS 102 231	R	
TSP postal address	According to TS 102 231	R	
TSP electronic address	According to TS 102 231	R	
TSP information URI	According to TS 102 231	R	
TSP information extensions	--	N	Not envisaged
Service Information			
Service type identifier	**"http://uri.spocs-eu.eu/Svctype/eDelivery/v1"** or **"http://uri.spocs-eu.eu/Svctype/eSafe/v1"** or **"http://uri.spocs-eu.eu/Svctype/PSC/v1"** or **"http://uri.spocs-eu.eu/Svctype/SC/v1"** or **"http://uri.spocs-eu.eu/Svctype/eSD/v1"** or **"http://uri.spocs-eu.eu/Svctype/searchModule/v1"** or **"http://uri.spocs-eu.eu/Svctype/syndica**	R	Will change after project conclusion, dependant on the chosen sustainability model. May include other service types if needed

Tag	Value	Required /Optional / NotUsed	Note
	tionModule/v1"		
Service name	According to TS 102 231	R	It is recommended to qualify the Service name with a domain name. This name is intended to be used for displaying.
Service digital identity	According to TS 102 231	R	Service X509 certificate. For eDelivery GWs this is the certificate used for signing evidences, messages and the SAML SenderVouches token. In cases where multiple certificates are necessary for different usages, the method shown below in Secion 2 MUST be used
Service current status	**"http://uri.etsi.org/TrstSvc/Svcstatus/inaccord"**	R	SPOCS TLS will only list "active" services, thus restricting the specification to the value "http://uri.etsi.org/TrstSvc/Svcstatus/inaccord"
Current status starting date and time	According to TS 102 231	R	UTC at which the current approval status became effective
Scheme service definition URI	According to TS 102 231	O	
Service supply points	According to TS 102 231	R	According to service type: PSC and eSafe: This URI must point to the SOAP address of the eSafe|PSC Info Service (getPscInfo or getESafeInfo) according the eSafe specification, where the PSC or eSafe portal can get further information of their communication partners eDelivery: URI for wsdl specification
TSP service definition URI	According to TS 102 231	O	

Tag	Value	Required /Optional / NotUsed	Note
Service information extensions	According to TS 102 231	R	Extensions depend on Service Type, see below: • Scheme extension for eDelivery provider • Scheme extension for eSafe provider • Scheme extension for PSC • Scheme extension for Service Catalogue • Scheme extension for eService Directory • Scheme extension for Service Catalogue • Scheme extension for eService Directorysyndication Module
Signature			
Scheme identification	<SPOCS TSL MAINTAINER public key>	R	Will change after project conclusion, dependant on the chosen sustainability model.
Signature algorithm identifier	According to TS 102 231	R	
Signature value	According to TS 102 231	R	
TSL extensions			
expiredCertsRevocationInfo Extension		N	Does not apply to services foreseen for SPOCS
additionalServiceInformation Extension		N	Does not apply to services foreseen for SPOCS

Table 2: SPOCS TSL elements profiling

2 Dealing with multiple certificates

If many certificates are needed for the definition of a service, the service will contain more entries in the element **`tsl:erviceDigitalIdentity`** . Every certificate will be characterized by a unique element **`sie:KeyUsageBit`**, which carries a **`@name`** attribute that qualifies the certificate with respect of its intended KeyUsage.

Note that this may not reflect the actual KeyUsage value of the certificate listed, encoded in the X509 format

Implementations will grant an ordered search to keep the association.

The **`KeyUsageBit`** attribute is defined as (e.g., for a certificate for non-repudiation):

```
<tsl:ServiceDigitalIdentity>
   <tsl:DigitalId>cert1</tsl:DigitalId>
   <tsl:Other>
      <sie:KeyUsage>
         <sie:KeyUsageBit name="nonRepudiation">
            true
         </sie:KeyUsageBit>
      </sie:KeyUsage>
   <tsl:Other>
<tsl:ServiceDigitalIdentity>
```

3 TSL scheme extensions

3.1 Scheme extension for eDelivery provider

For each eDelivery Gateway the following extension information MUST be provided within the **ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl ServiceInformationExtensions/
            tsl:Extension/
               stsl:TSLeDeliveryExtension
```

Mandatory information:

- Realm name (e.g.: “OSCI”, “PEC”, ….) – more Gateways may be deployed for a single realm
- Gateway country code (when applicable)
- Managed Domain list (this might be a very long list, for Italy it will include 5.000 2nd and 3rd level domains like <“legalmail.it”, “ulss8.legalmail.it”, “postecom.it”, …>)
- List of supported e-address schemas (see section 3.3 for details).
- List of provided evidences (e.g: <“SubmissionAcceptanceRejection”, “RelayToREMMDAcceptanceRejection”, “RelayToREMMDFailure”, …>)
- List of evidences to be made available with Dispatch submission from source Gateway (applicable only <“SubmissionAcceptanceRejection”, “ReceivedFromNonREMSystem">)
- Supported authentication levels

3.2 Scheme extension for eSafe provider

For each eSafe service the following extension information MUST be provided within the the **ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl:ServiceInformationExtensions/
            tsl:Extension/
               stsl:TSLeSafeExtension
```

Mandatory information:

- Service country code (when applicable): This attribute according to the standard ISO 3166-1 allows the PSC portal to offer a preselected list of available eSafes in the users home country
- Service working mode (Push/Pull)
- Supported authentication levels

3.3 Scheme extension for PSC

For each PSC service the following extension information MUST be provided within the **tsl:ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl:ServiceInformationExtensions/
            tsl:Extension/
               stsl: TSL_PSC_Extension
```

Mandatory information:

- Service country code
- Supported authentication level

3.4 Scheme extension for Service Catalogue

For each Service Catalogue (eSC) the following extension information MUST be provided within the **tsl:ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl: ServiceInformationExtensions/
            tsl:Extension/
               stsl: TSL_SC_Extension
```

Mandatory information:

- Service country code
- Supported authentication level

It should be remarked that information on the TSL relates to the SCs themselves (as service providers), not to the services they list.

3.5 Scheme extension for eService Directory

For each eService Directory (eSD) the following extension information MUST be provided within the **tsl:ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl: ServiceInformationExtensions/
            tsl:Extension/
               stsl: TSL_eSD_Extension
```

Mandatory information:

- Service country code
- Supported authentication level

It should be remarked that information on the TSL relates to the eSDs themselves (as service providers), not to the services they list.

3.6 Scheme extension for searchModule

For each search Module the following extension information MUST be provided within the **tsl:ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl: ServiceInformationExtensions/
            tsl:Extension/
               stsl: TSL_searchModule_Extension
```

Mandatory information:

- Service country code

3.7 Scheme extension for syndicationModule

For each syndication Module the following extension information MUST be provided within the **tsl:ServiceInformationExtensions** node, in a subtree containing the elements shown below:

```
tsl:ServiceInformation/
      tsl: ServiceInformationExtensions/
            tsl:Extension/
               stsl: TSL_syndicationModule_Extension
```

Mandatory information:

- Service country code

3.8 XML schema for service information extension

According to TS 102 231, service level extensions are defined within the **`tsl:ServiceInformationExtensions`** element, as a sequence of **`tsl:Extension`**.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:stsl="http://uri.eu-spocs.eu/tsl/v1#" xmlns:tsl="http://uri.etsi.org/02231/v2#"
   xmlns:xml="http://www.w3.org/XML/1998/namespace" xmlns:rem="http://uri.etsi.org/02640/v1#"
   targetNamespace="http://uri.eu-spocs.eu/tsl/v1#" elementFormDefault="qualified"
   attributeFormDefault="unqualified">
   <xs:import namespace="http://uri.etsi.org/02640/v1#"
      schemaLocation="ts102640_v1.xsd" />
   <xs:import namespace="http://uri.etsi.org/02231/v2#"
      schemaLocation="http://uri.etsi.org/02231/v3.1.2/ts_102231v030102_xsd.xsd" />
   <xs:complexType name="TSLeDeliveryExtensionType" mixed="true">
      <xs:sequence>
         <xs:element name="eDeliveryRealmName" type="xs:string" />
         <xs:element name="countryCode" type="tsl:SchemeTerritoryType" />
         <xs:element name="supported_eAddressSchemas" type="stsl:supported_eAddressSchemasType" />
         <xs:element name="managedDomains" type="stsl:managedDomainListType" />
         <xs:element name="supportedAuthenticationLevels" type="stsl:supportedAuthLevelsType" />
         <xs:element name="supportedEvidenceList" type="stsl:supportedEvidenceListType" />
         <xs:element name="requestedEvidenceList" type="stsl:supportedEvidenceListType" />
      </xs:sequence>
   </xs:complexType>
```

```
<xs:complexType name="managedDomainListType">
   <xs:sequence>
      <xs:element name="managedDomain" type="xs:string"
         minOccurs="0" maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>
<xs:element name="TSLeDeliveryExtension" type="stsl:TSLeDeliveryExtensionType" />
<xs:complexType name="supportedEvidenceListType">
   <xs:sequence>
      <xs:element name="supportedEvidence" minOccurs="0"
         maxOccurs="unbounded">
         <xs:simpleType>
            <xs:restriction base="tsl:NonEmptyURIType">
               <xs:enumeration
                  value="http:uri.etsi.org/REM/Evidence#SubmissionAcceptanceRejection" />
               <xs:enumeration
                  value="http:uri.etsi.org/REM/Evidence#RelayREMMDAcceptanceRejection" />
               <xs:enumeration value="http:uri.etsi.org/REM/Evidence#RelayREMMDFailure" />
               <xs:enumeration
                  value="http:uri.etsi.org/REM/Evidence#DeliveryNonDeliveryToRecipient" />
               <xs:enumeration
                  value="http:uri.etsi.org/REM/Evidence#RetrievalNonRetrievalByRecipient" />
               <xs:enumeration
                  value="http:uri.etsi.org/REM/Evidence#ReceivedFromNonREMSystemReceivedFromNonREMSystem" />
            </xs:restriction>
         </xs:simpleType>
```

```
         </xs:element>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="supported_eAddressSchemasType">
      <xs:sequence>
         <xs:element name="supported_eAddressSchema" type="tsl:NonEmptyString"
            minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="supportedAuthLevelsType">
      <xs:sequence>
         <xs:element name="supportedAuthLevel" minOccurs="0"
            maxOccurs="unbounded">
            <xs:simpleType>
               <xs:restriction base="tsl:NonEmptyURIType">
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#Basic" />
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#Enhanced" />
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#Strong" />
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#AdES" />
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#AdES-Plus" />
                  <xs:enumeration value="http:uri.etsi.org/REM/AuthMethod#QES" />
               </xs:restriction>
            </xs:simpleType>
         </xs:element>
      </xs:sequence>
   </xs:complexType>
```

```
<xs:complexType name="supportedIdSchemasType">
   <xs:sequence>
      <xs:element name="supportedIdSchema" type="tsl:NonEmptyString"
         minOccurs="0" maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>
<xs:complexType name="TSLeSafeExtensionType" mixed="true">
   <xs:sequence>
      <xs:element name="countryCode" type="tsl:SchemeTerritoryType" />
      <xs:element name="supportedIdSchemas" type="stsl:supportedIdSchemasType" />
      <xs:element name="supportedAuthenticationLevels" type="stsl:supportedAuthLevelsType" />
      <xs:element name="eSafeoperationMode" type="stsl:eSafeOperationModeType" />
   </xs:sequence>
</xs:complexType>
<xs:element name="TSLeSafeExtension" type="stsl:TSLeSafeExtensionType" />
<xs:complexType name="eSafeOperationModeType">
   <xs:sequence>
      <xs:element name="eSafeOperationMode" type="xs:string"
         minOccurs="0" maxOccurs="unbounded" />
   </xs:sequence>
</xs:complexType>
<xs:complexType name="TSL_PSC_SC_eSD_ExtensionType"
   mixed="true">
   <xs:sequence>
      <xs:element name="countryCode" type="tsl:SchemeTerritoryType" />
      <xs:element name="supportedAuthenticationLevels" type="stsl:supportedAuthLevelsType" />
```

```
      </xs:sequence>
   </xs:complexType>
   <xs:element name="TSL_PSC_Extension" type="stsl:TSL_PSC_SC_eSD_ExtensionType" />
   <xs:element name="TSL_SC_Extension" type="stsl:TSL_PSC_SC_eSD_ExtensionType" />
   <xs:element name="TSL_eSD_Extension" type="stsl:TSL_PSC_SC_eSD_ExtensionType" />
   <xs:element name="TSL_searchModule_Extension" type="stsl:TSL_PSC_SC_eSD_ExtensionType" />
   <xs:element name="TSL_syndicationModule_Extension" type="stsl:TSL_PSC_SC_eSD_ExtensionType" />
</xs:schema>
```

References

[1] RFC 2119: Key words for use in RFCs to Indicate Requirement Levels; http://tools.ietf.org/html/rfc2119 (last visited on 08th May 2010)

[2] RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types; http://tools.ietf.org/html/rfc2046 (last visited on 08th May 2010)

[3] XML Signature Syntax and Processing (Second Edition): http://www.w3.org/TR/xmldsig-core/ (last visited on 08th May 2010)

[4] RFC 1951: DEFLATE Compressed Data Format Specification version 1.3; http://tools.ietf.org/html/rfc1951 (last visited on 08th May 2010)

[5] W3C Recommendation Web Services Addressing 1.0; http://www.w3.org/TR/ws-addr-core/ (last visited on 08th May 2010)

[6] OASIS Standard WS-Security; http://www.oasis-open.org/specs/index.php#wssv1.1 (last visited on 08th May 2010)

[7] SPOCS Project, D3.1 "Assessment of eDelivery systems and specifications required for interoperability", http://www.eu-spocs.eu/index.php?option=com_processes&task=showDocument&did=198&id=18&Itemid=1 (last visited on 20th May 2010)

[8] SPOCS Project, D5.2 parts "Functional requirements for WP3 eDelivery" and "Functional requirements for WP3 eSafe", not yet published

[9] ETSI TS 102 231, v3.1.2, Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information; http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf (last visited on 20th May 2010)

[10] PEPPOL Deliverable D1.1 Requirements for Use of Signatures in Public Procurement Processes, Part 4: Architecture and Trust Models; http://www.peppol.eu/work_in_progress/wp-1-esignature/results/d1-1-part-4-architecture-and-trust-models (last visited on 20th May 2010)

[11] PEPPOL BusDox v. 1.0 specifications, http://www.peppol.eu/work_in_progress/wp8-Solutions%20architecture %2C%20design%20and%20validation/specifications/v1-0-specifications (last visited on 21th May 2010)

[12] ETSI TS 102 640-2, Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats and Policies; Part 2: Data Requirements and Formats for Signed Evidences for REM; http://www.etsi.org/deliver/etsi_ts/102600_102699/10264002/02.01.01_60/ts_10264002v020101p.pdf (last visited on 21th May 2010)

[13] SOAP Message Transmission Optimization Mechanism, W3C Recommendation 25 January 2005, http://www.w3.org/TR/soap12-mtom/

[14] SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation 27 April 2007, http://www.w3.org/TR/soap12-part1/

[15] Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.2, OASIS Standard, 2 September 2003, http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf, (last visited on 21th May 2010)

[16] Web Services Addressing 1.0 – SOAP Binding, W3C Recommendation 9 May 2006, http://www.w3.org/TR/2006/REC-ws-addr-soap-20060509/, (last visited on 21th

May 2010)

[17] Web Services Security SAML Token Profile 1.1, OASIS Standard Specification incorporating Approved Errata, 1 November 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SAMLTokenProfile.pdf, (last visited on 21th May 2010)

[18] Web Services Security X.509 Certificate Token Profile 1.1, OASIS Standard Specification, incorporating Approved Errata, 1 November 2006, http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-x509TokenProfile.pdf, (last visited on 21th May 2010)

[19] World Wide Web Consortium. XML Encryption Syntax and Processing, W3C Recommendation, 10.12.2002; http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, (last visited on 21th May 2010)

[20] World Wide Web Consortium. Extensible Markup Language (XML) 1.0 (Fourth Edition), T. Bray, J. Paoli, C. M. Sperberg-McQueen, and E. Maler, Editors. 10 February 1998, revised 16 August 2006; http://www.w3.org/TR/2006/REC-xml-20060816/, (last visited on 21th May 2010)

[21] RFC 2368, The mailto URL scheme; http://www.rfc-editor.org/rfc/rfc2368.txt

[22] RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1; http://www.rfc-editor.org/rfc/rfc2616.txt, (last visited on 21th May 2010)

[23] RFC 2817, Upgrading to TLS Within HTTP/1.1; http://tools.ietf.org/html/rfc2817, (last visited on 21th May 2010)

[24] RFC 4122, A Universally Unique Identifier (UUID) URN Namespace, The Internet Engeneering Task Force July 2005, http://www.ietf.org/rfc/rfc4122.txt, (last visited on 21th May 2010)

[25] OSCI-Transport - Version 2.0, Edition 3 - Web Services Profiling and Extensions Specification, OSCI Steering Office 2010, http://www.osci.eu/transport/osci20/20100427/OSCI20_WS-ProfilingAndExtensionSpecification_Edition3.pdf, (last visited on 21th May 2010)

[26] RFC 822, Standard for the format of ARPA Internet text messages, The Internet Engeneering Task Force August 1982, http://www.ietf.org/rfc/rfc0822.txt, (last visited on 21th May 2010)

[27] ETSI TS 101 903: XML Advanced Electronic Signatures, V1.4.1 2009-06; http://pda.etsi.org/exchangefolder/ts_101903v010401p.pdf (last visited on 9th July 2010)

[28] RFC 822, Standard for the format of ARPA Internet text messages, The Internet Engineering Task Force August 1982, http://www.ietf.org/rfc/rfc0822.txt, (last visited on 21th May 2010)

[29] WS-I Basic Profile 2.0, Working Group Draft, 2007-10-25, Web Services Interoperability Organization, http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html, (last visited on 19th July 2010)

[30] SOAP Message Transmission Optimization Mechanism, W3C Recommendation 25 January 2005, http://www.w3.org/TR/soap12-mtom/ (last visited on 27th July 2010)

[31] XML Binary Optimized Packaging, W3C Recommendation 25 January 2005, http://www.w3.org/TR/xop10/ (last visited on 27th July 2010)

[32] RFC 5322: Internet Message Format; http://tools.ietf.org/html/rfc5322 (last visited on 28th July 2010)

[33] Describing Media Content of Binary Data in XML, W3C Working Group Note, 5 May 2005, http://www.w3.org/TR/xml-media-types/ (last visited on 29th July 2010)

[34] RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax, http://www.ietf.org/rfc/rfc2396.txt, (last visited on 11th August 2010)

[35] STORK D5.1.8.b - Interface Specification, 31/7/2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=960 (last visited on 08th August 2010)

[36] STORK D6.4.1 - eDelivery Functional Specification, 08/11/2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=971 (last visited on 08th August 2010)

[37] ISO 3166-1 Country Codes, Version2006, lat update 2009-10-23, http://www.tm-xml-wiki.org/wiki/TM-XML_ISO_3166_Country_Code_XSD (last visited on 18th August 2010)

[38] STORK D2.3 - STORK Quality authenticator scheme, 2009-03-03, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=577 (last visited on 18th August 2010)

[39] Secure Hash Standard, Federal Information Processing Standards Publication 180-2 (extended to include SHA-384, SHA-256, and SHA-512), 2002 August 1, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf (last visited on 27th August 2010)

[40] RFC 4051, Additional XML Security Uniform Resource Identifiers, D. Eastlake 3rd, April 2005, http://www.ietf.org/rfc/rfc4051.txt (last visited on 27th August 2010)

[41] XML Signature Syntax and Processing Version 1.1, W3C Working Draft 04 February 2010, D. Eastlake 3rd et. al., http://www.w3.org/TR/2010/WD-xmldsig-core1-20100204/ (last visited on 27th August 2010)

[42] RFC3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, J. Jonsson et.al., http://www.ietf.org/rfc/rfc3447.txt (last visited on 27th August 2010)

[43] Specification for the Advanced Encryption Standard AES), 26 November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (last visited on 27th August 2010)

[44] eps e-payment standard Pflichtenheft V2.3, Joachim Geisler, Christian Matschi, March 2009, http://www.stuzza.at/1111_DE.6488C3D06b0d1db8f99c75d5082dbde7c4e3fa71 (last visited on 27th August 2010)

[45] ETSI TS 102 640-4, Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM_MD Conformance Profiles; http://www.etsi.org/deliver/etsi_ts/102600_102699/10264004/02.01.01_60/ts_10264004v020101p.pdf (last visited on 21th May 2010

All following documents of SPOCS D 2.2 and D3.2 are finalized on 30 September 2010 and will be published after approval through the EC[1]:

[46] SPOCS D2.2 Standard Document and Validation Common Specifications"

[47] SPOCS D3.2 Functional Specification, Architecture and Trust Model

[1] Meanwhlie available at:

http://www.eu-spocs.eu/index.php?option=com_processes&task=streamFile&id=18&fid=699

[48] Appendix 1: Security Architecture Development Process

[49] Appendix 2: Trust-service Status List Profiling ("SPOCS TSL")

[50] Appendix 3: eDelivery Interconnect Protocol and Gateway Specification

[51] Appendix 4: eSafe – Operations in Detail

[52] Appendix 5: SPOCS TSL Accreditation and Operation Policy

[53] Appendix 6: Security Model