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 5: SPOCS TSL Accreditation and Operation Policy

Deliverable Id :	D3.2
Deliverable Name :	SPOCS TSL Accreditation and Operation Policy
Status :	Draft 0.9
Dissemination Level :	SPOCS internal and EU Commission
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):	Michael Seeger (DE Siemens)
Partner(s) contributing :	SPOCS.AT, DE BVA, DE Siemens, GR MINT, IT InfoCamere, NL MINEZ, PL ILIM

Abstract: This document Appendix 5 is part of the second deliverable in work package 3 of the EU co-funded project SPOCS. It describes the SPOCS TSL Accreditation and Operation Policy required to provide secure operation and accreditation of SPOCS services to the SPOCS-TSL to ensure the reliability and trustworthiness of the SPOCS-TSL as a fundamental cornerstone of the security architecture.

History

Version	*Date*	*Modification reason*	*Modified by*
0.1		Initial draft	Seeger
0.2	24/08/2010	Reformatting and first review	Seeger
0.9	14/09/2010	Aligned and finalized; ready for QA	Seeger

Table of contents

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.

- **Fehler! Verweisquelle konnte nicht gefunden werden.** is accomplished by following separated appendix documents:
- **Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Fehler! Verweisquelle konnte nicht gefunden werden.**
- **Fehler! Verweisquelle konnte nicht gefunden werden.**.

This document Appendix 5: SPOCS TSL Accreditation and Operation Policy is part of the second deliverable of SPOCS WP3.

Used abbreviations, general document conventions as well as referenced XML namespaces are outlined in the main document **Fehler! Verweisquelle konnte nicht gefunden werden.** while the overall reference list is contained in every separate appendix document, too.

1 Scope and Structure of This Document

This Policy regulates the Operation of the SPOCS-TSL and the according Accreditation process. It does particularly list requirements that apply to both the SPOCS-TSL issuer as well as a SPOCS trusted service listed as such in the SPOCS-TSL

This policies is explicitly aligned with ETSI TS 102 640-3 as services that are subject to ETSI TS 102 640-3 are also within the scope of this document. To prevent collisions and discrepancies this policy does where ever possible adopt the formulations of ETSI TS 102 640-3.

Furthermore it should be explicitly stated that this policy is subject to change as other EU Projects like PEPPOL and BusDOCS need to be aligned too. As those projects have not yet decided on corresponding policies alignment with them had to be postponed.

1.1 Definitions and abbreviations

1.1.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 640-1 [i.1] and the following apply:

- information security management system: part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

  NOTE: See ISO/IEC 27001 [1], clause 3.7.

- The keywords “must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" used in this document are to be interpreted as described in RFC 2119 http://tools.ietf.org/html/rfc2119 (last visited on 20th August 2010)

1.1.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

(**Note:** Some of the abbreviations used in this appendix differ from the usage in the main document)

CA	Certification Authority
ISMS	Information Security Management System
REM	Registered E-Mail
REM-MD	REM Management Domain
UTC	Coordinated Universal Time
WORM	Write Once Read Many
SPOCS	Simple Procedures Online for Cross-border Services

2 Trust Models and Trust Requirements

For trust to be established and formally instantiated by means of a "trusted list of services" it is essential that each component within the chain of trust is indeed trust worthy. The next chapters will further specify different aspects essential for formation of trust.

2.1 Levels of Trust

Generally speaking trust has two main components:

1. "Technical trust" in the technology used, i.e. computer systems and the means to communicate between these systems.
2. "Organizational trust" between the actors that eventually shall carry out the business transactions, e.g. enter a contractual relationship.

For a service like eSafe or eDelivery to be listed as a trusted service in the SPOCS-TSL the technical level is mainly about:

- Compliance with the SPOCS specification for the respective service
- Compliance with a SPOCS operational policy

- The second level in general requires more than technical measures but includes
- Audit of compliance against SPOCS operational policy
- Policy for enforcement of compliance, including sanctions like blacklisting
- Criteria for accreditation including
    - trustworthiness and honesty of purpose
    - credit rating
    - legal liability clauses
    - legislation for oversight

SPOCS however may only propose a limited subset of criteria and point to action items that must be addressed otherwise.

2.2 Trust Anchors for Services and Authorities

For the SPOCS-TSL to act as an authoritative inventory of SPOCS trusted services both to SPOCS infrastructure components as well as to consumers obviously the SPOCS-TSL root certificate must be known to the relying party and must be verifiably valid. This means that the SPOCS-TSL issuer must use a certificate to sign the SPOCS-TSL that was issued by a Certificate Authority that is listed at least in one national TSL or a central European TSL.

This certificate should be a qualified certificate as defined in RFC 3739/ ETSI TS 101 862 which automatically means that there needs to be a physical human person that signs responsible for the formal correctness of the SPOCS-TSL and takes legal responsibility. If non qualified certificate are used those shall be issued by a governmental institution, responsible for supervision and accreditation of service providers.

Every SPOCS service that wants to accreted as a "SPOCS trusted service" should be in possession of a certificate that satisfies ETSI TS 101 862 (this might implicate that the certificate is issued on an identifiable alias indicating that a natural person is acting on behalf of a service). The certificate may be subject to TS 101 456 §8. Self signed certificates are not accepted.

2.3 Accreditation process

Each SPOCS service that applies to be listed as a "SPOCS trusted service" in the SPOCS-TSL must explicitly consent to and be compliant with this policy.

The .SPOCS-TSL issuer shall in particular:

- Confirm by telephone, confirmatory postal mail, or comparable procedure to the applicant certain information about the organization, that the organization has authorized the Trusted Service list application and that the person submitting the Trusted Service list application on behalf of the Trusted Service list Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the organization, the employment of that individual and his/her authority to act on behalf of the organization shall also be confirmed.
- Check that the Subject named in the certificate is actively engaged in running the service
- Check that the Applicant has its jurisdiction of incorporation or registration or place of business not in any country with which the laws of the SPOCS-TSL issuer's jurisdiction prohibit doing business
- Check for Government Agencies applying to operate a SPOCS trusted service:
    - Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates, check Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity.
- Check for Business Entities applying to operate a SPOCS trusted service:
    - Verify that the Entity is engaged in business under the name submitted by Applicant in the Application. Check that the certificate used for incorporation in the SPOCS-TSL matches with Applicant's formal legal name, or if a qualified certificate is used that the person named in the qualified certificate is authorized to act on behalf of the Applicant. Check with the competent Registration Agency in Applicant's Jurisdiction of Registration.
- Check for International Non-Commercial Entities applying to operate a SPOCS trusted service:
    - Verify that Applicant is a legally recognized International Organization Entity.
    - Check that the certificate used for incorporation in the SPOCS-TSL matches with Applicant's formal legal name, or if a qualified certificate is used that the person named in the qualified certificate is authorized to act on behalf of the Applicant.
    - Check Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity.

The SPOCS trusted service Applicant shall in particular:

- Contractually agree to be compliant with this policy
- Announce termination of service without any undue delay to the SPOCS-TSL issuer.
- Notify the SPOCS-TSL issuer without undue delay of any security breach affecting applying Service.

Circumstances for Revocation and Suspension

The status of SPOCS trusted service and inclusion in the SPOCS-TSL must be revoked if the SPOCS-TSL issuer

- becomes aware that the Service does not comply with applicable laws
- That the Service is not trustworthy, honest, or reputable in its business dealings; does not comply with this policy or has its Jurisdiction of Incorporation or Registration or Place of Business in any country with which the laws of SPOCS-TSL issuer's jurisdiction prohibit doing business
- Is insolvent, applied for creditor protection or is otherwise liquidated

The status of SPOCS trusted service and inclusion in the SPOCS-TSL shall be suspended if the SPOCS-TSL issuer

- Becomes aware of a security breach in the Service

3 Requirements for Operation

The requirements for operation of a SPOCS trusted service may be differentiated in general requirements, like an information security policy, and more specific requirements, like compliance to a certain ETSI spec for REM. Compliance with all these requirements is a mandatory prerequisite for being successfully accredited.

3.1 General requirements

3.1.1 Information security management systems for the operation of SPOCS “trusted services”

Information, like other organization assets, is an essential contributor to an organization's business. Regardless of the form or functionality of the information, or the means by which the information is shared or stored, information should always be appropriately protected.

Therefore, it is essential for an organization to ensure its information security by continuously improving information security management system (ISMS) in accordance with ISO/IEC 27001 [1]. In addition, as some SPOCS infrastructure components have specific security objective regarding authenticity and integrity of “evidence attestations” and non repudiatability specific policy objectives and controls need to be applied to address known threats to such objectives.

Information systems and networks are subject to a broad set of security threats including computer-assisted fraud, espionage, sabotage, and vandalism, unauthorized modification of evidence and leakage of personal message information. These threats may originate from inside or outside the operating organizations. Once information security is violated, for example by leakage of personal data or tampering with evidence, user confidence in the SPOCS infrastructure will suffer major damage. Furthermore, the resulting impact on the user's business and potentially a critical element of national infrastructure (secure messaging services) could be significant.

An Information Security Policy is a statement of policy which provides management direction and support for information security in accordance with business requirements and relevant laws and regulations. It is one of the fundamental components of an Information Security Management System based on ISO/IEC 27001 [1]. An Information Security Policy is concerned with information security rather than the specific requirements of SPOCS. Every operator of a SPOCS trusted service must have an Information Security Policy.

A SPOCS service policy governs and regulated the general operation of SPOCS infrastructure services.

3.1.2 Security Risk Assessment

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business impact likely to result from security failures. The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

For general guidance on establishing security requirements and assessing security risks see ISO/IEC 27005 [4.1]

3.1.2.1 Control Selection

Once threats, vulnerabilities and associated risks have been identified appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level.

The present document provides recommended controls for SPOCS based on the controls recommended in

ISO/IEC 27002 [2] adapted to meet the specific requirements.

The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, and the general risk management approach and must be aligned with national and international legislation and regulatory standards.

Control selection should especially target to meet the following security objectives:

- CON_BIZ: Confidentiality of strategic business planning information of SPs
  - between SP and PSC (mandatory, this is in the SPOCS focus)
  - between SP and CA (recommended, but not governed by SPOCS)
- CON_PID: Confidentiality of PID (personally identifiable data) of SPs
  - between SP and PSC (mandatory, this is in the SPOCS focus)
  - between SP and CA (recommended, but not governed by SPOCS)
- INT_PID: Integrity of personally identifiable data of SPs
  - between the SP and PSC (mandatory, this is in the SPOCS focus)
  - between SP and CA (recommended, but not governed by SPOCS)
- AUT_PID: Authenticity of PID, current and in long-term retrospective (e.g. for forensics)
- AV_PID: Availability of PID
- CON_DOC: Confidentiality of submitted documents of the SPs
  - between SP and PSC (mandatory, this is in the SPOCS focus)
  - between SP and CA (recommended, but not governed by SPOCS)
- INT_DOC: Integrity of submitted documents of the SPs
  - between the SP and PSC (mandatory, this is in the SPOCS focus)
  - between SP and CA (recommended, but not governed by SPOCS)
- AUT_DOC: Authenticity of submitted documents of the SPs
- AV_DOC: Availability of submitted documents of the SPs
- NR_DOC: Non-repudiation of submitted documents
- TS_DOC: Authentic time stamps on submitted documents
- RET_DOC: Compliance with Retention time legislation for submitted documents of the SPs (recommended, but not governed by SPOCS)
- CON_DEC: Confidentiality of official notifications on CA decisions
  - between PSC and SP (mandatory, this is in the SPOCS focus)

    - between CA and SP (recommended, but not governed by SPOCS)
- INT_DEC: Integrity of official notifications on CA decisions
    - between PSC and SP (mandatory, this is in the SPOCS focus)
    - between CA and SP (recommended, but not governed by SPOCS)
- AUT_DEC: Authenticity of official notifications on CA decisions
- AV_DEC: Availability of official notifications on CS decisions
- NR_DEC: Non-repudiation of official notifications on CA decisions
- TS_DEC: Authentic time stamps on official notifications on CA decisions
- RET_DEC: Compliance with Retention time legislation for official notifications on CA decisions (recommended, but not governed by SPOCS)

3.1.2.2 Application of ISO/IEC 27002 Controls and Objectives

The controls specified in ISO/IEC 27002 [2] shall be applied by an ISMS conforming to ISO/IEC 27001 [1] taking into account the following.

3.1.2.2.1 Security Policy

Controls under clause 5 from ISO/IEC 27002 [2] apply. A SPOCS service shall establish, implement, operate, monitor, review, maintain and improve a documented Information Security Management System as specified in ISO/IEC 27001 [1], applying the controls identified in this clause and, as determined through ISMS, ISO/IEC 27002 [2], taking into account the additional points identified in clause 6.

3.1.2.2.2 Organization of information security

Controls under clause 6.1 from ISO/IEC 27002 [2] apply.

Controls under clauses 6.2.1 and 6.2.2 from ISO/IEC 27002 [2] apply.

In the context of clause 6.2 of ISO/IEC 27002 [2]:

- In order to maintain security with external parties SPOCS service shall also make available a SPOCS service practices statement to all relying parties as specified in clause 6.1
- When interconnecting with other SPOCS infrastructure services contractual agreement shall be defined as specified in clause 6.2.

3.1.2.2.3 Asset management

Controls under clause 7 from ISO/IEC 27002 [2] apply, in particular for Evidence.

3.1.2.2.4 Human resources security

Controls under clause 8 from ISO/IEC 27002 [2] apply.

3.1.2.2.5 Physical and environmental security

Controls under clause 9 from ISO/IEC 27002 [2]apply.

3.1.2.2.6 Communications and operations management

Controls under clause 10 from ISO/IEC 27002 [2] apply. In particular, clocks of all SPOCS systems which shall be synchronized with UTC (if required with local offset which shall be recorded in the REM Practice statement) within 1 minute.

3.1.2.2.7 Access control

Controls under clause 11 from ISO/IEC 27002 [2] apply.

In particular,

- eDelivery Senders and eDelivery Recipients shall be authenticated as specified in clause 6.3 of the present document.
- All administrative access of operating stuff shall be strongly authenticated

3.1.2.2.8 Security requirements of information systems

Controls under clause 12 from ISO/IEC 27002 [2] apply. In particular, in relation to cryptographic controls specified in clause 12.3 of ISO/IEC 27002 [2], electronic signatures shall be applied as specified in clause 6.4.

3.1.2.2.9 Information security incident management

Controls under clause 13 from ISO/IEC 27002 [2] apply.

3.1.2.2.10 Business continuity management

Controls under clause 14 from ISO/IEC 27002 [2] apply.

3.1.2.2.11 Compliance

Controls under clause 15 from ISO/IEC 27002 [2] apply. In particular:

- in the context of clause 15.1.3 the integrity of eDelivery Evidence shall be preserved as specified in clause 6.5;
- in the context of clause 15.1.3 records shall be destroyed as specified in clause 6.6
- in the context of clause 15.2 any SPOCS Policy applicable to the eDelivery shall be applied.

3.2 Further Requirements

The following controls shall be applied within the context of the ISO/IEC 27002 [2] requirements as specified above.

3.2.1 SPOCS Practice Statement

The SPOCS Practice Statement is a statement of the practices employed in providing SPOCS services meeting the policy requirements specified in the present document. The SPOCS Practice statement shall include as applicable, at least:

- Specification of the country/ies under whose legal system the SPOCS service operates and other applicable legal requirements (where applicable)
- Reference to SPOCS Policy or other legal or policy requirements to which the SPOCS service conforms; Details of any certification of conformance, government accreditation or other form of external audit against the requirements specified in the present document.
- The Style(s) of Operation the SPOCS service implements.

- Specification on the hashing algorithm (e.g. "SHA-1", "SHA256") currently used in the service. It may specify also the previously adopted hashing algorithms, also indicating the time period they have been in force.
- Information on how the requirements specified in the present document are implemented, including at least:
    - a statement of applicability of the ISO/IEC 27002 [2] controls taking into account the particular requirements specified in the present document;
    - whether Advanced signatures are supported by Qualified Certificates in accordance with Directive 1999/93/EC [4];
    - the level of authentication required by eDelivery Sender and eDelivery Recipients (see clause 6.3);
    - the period of time for which records are kept.
    - the offset from the UTC time specified in Evidence, Headers, etc..

Obligations to be met by the Service, including:

- protect any keys, password or other objects used for authentication purposes;.

Obligations to be met by any party relying on SPOCS TSL, including:

- verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying parties in the related CA's Certificate Policy and/or Certificate Practice Statement;

NOTE: take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate itself or in the terms and conditions supplied by the certificate issuing CA;

3.2.2 SPOCS Interconnection Statement

The SPOCS Interconnection statement is an agreement between SPOCS infrastructure components and services defining the controls to be applied to protect data exchanged between the SPOCS infrastructure components and services

Each SPOCS infrastructure components and services shall abide by the SPOCS Interconnection statements it is bound to by the above mentioned agreements or statement of policy.

3.2.3 eDelivery Sender/eDelivery Recipient Authentication

eDelivery Senders and eDelviery Recipients, as identified in eDelivery Evidence, shall be authenticated in one of the following ways:

- Basic: using basic authentication mechanisms such as passwords (The user may authenticate using
- passwords only if protected and only if used with an authenticated server. (e.g. using TLS/SSL);
- Enhanced: using enhanced authentication such

  as two factor authentication mechanisms linked

  to a one time password;
- Strong: mutual SSL authentication, which includes client's side user certificate;
- AdES: using advanced electronic signatures;
- AdES-Plus: using advanced electronic signatures with Secure Signature Creation Devices (as defined in Directive 1999/93/EC [4]) or equivalent secure cryptographic device;
- QES: using advanced electronic signatures with Secure Signature Creation Devices and Qualified Certificates (as defined in Directive 1999/93/EC [4]). The form of authentication used shall be documented in the SPOCS Practice Statement. NOTE: See also TS 102 640-2 [i.2], clause on "REM Sender/Recipient authentication details".

3.2.4 Electronic Signatures

3.2.4.1 Class of Electronic Signature

A class of electronic signature shall be employed that assures the authenticity and integrity, and where applicable commitment to content, over the lifetime of eDelivery Evidence and eDelivery Envelopes and other SPOCS service messages..
The signature shall be at least an Advanced Electronic Signature, as defined in Directive 1999/93/EC [4]. The signature shall be created using a Secure Signature Creation Devices1 and may be supported by Qualified Certificates (as defined in Directive 1999/93/EC [4]).

The form of signature used shall be document in the REM Practice Statement.

3.2.4.2 Public Key Certificates

Certificates shall be obtained from authorities who can reliably certify public keys

[1] For the use of „secure signature creation devices in automated processing please consider http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd4.pdf p.55 and

"The legislator assumes secure signature-creation devices to be constructed in a way that regularly offers a user the option to authenticate before each single signature or to authenticate once before creating a certain number of signatures or before the creation of signatures within a certain timeframe. Therefore, the creation of more than one electronic signature after a single authentication process is legal, if the automatic process ensures protection against misuse." (Waldeck, Frankfurt 2005). The use of secure signature creation devices for automated processing should be carefully considered by each Service for compliance with its governing legislation. We explicitly make no legally binding provision about usability.

and maintain revocation status information.

REM-MD Evidence and REM-MD Envelope signatures, if applicable, shall be supported by one of the following:

- Certificates issued by CAs that operate under certificate policies as per TS 102 042 [5] (NCP+ type) or policies and practices that are nationally recognized by the applicable regulations as being sufficiently reliable for the purposes of REM;
- Qualified certificates issued by CAs that operate under qualified certificate policies as per TS 101 456 [6] (include requirements for the use of SSCD) or practices that are nationally recognized for issuing qualified certificates;
- The operation of the CA supporting REM-MD signatures shall be independent of the REM-MD.

3.2.4.3 Protection of Private Signing Key

The private signing key used to sign REM-MD Evidence and REM-MD Envelopes shall be generated and kept secure

in controlled circumstances.
The key used to sign REM-MD Evidence and REM-MD Envelopes shall be held and used within a secure signature creation device which:

- meets the requirements identified in FIPS PUB 140-2 [10] level 3 or higher; or
- is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8]; or
- it is assured to any comparable criteria recognized in the specific EU Member State.

3.2.5 Records Retention and Destruction

Records shall be kept relating to the provision of SPOCS services, including audit logs and SPOCS eDelivery Evidence, for the period required to support local law and any agreement with other SPOCS services, by means that maintains their authenticity and integrity over the required period, in compliance with the Personal Data Protection legislation. In particular, any personal data shall be destroyed when no longer required, unless differently agreed upon with the users or required by the applicable legislation.

3.2.6 Requirements for the administration of interoperability framework components

Without accompanying secure operational procedures and respective security governance every security architecture remains ephemeral. More over some aspects of a security architecture are not so much a technological solution but must be solved on a process level. A good example is “trust levels”. Without proper contracts and service level agreements establishing trust only by technical means can not succeed.

General operational and security requirements

The following table provides a list of additional security controls that need to be implemented in order to fulfil the accreditation process criteria.

3.2.6.1 Non technical

- All components accessible to end users (Service Providers) shall implement clear and understandable privacy policy and make them accessible to the user. This privacy policy shall obey to the principle of data reduction and implement an "opt-in" policy for all further use
- All components accessible to end users (Service Providers) shall implement clear and understandable service level agreements and make them accessible to the user
- Changes to the framework must be evaluated on the impact on security.
- The framework must periodically be subjected to a security penetration test.
- Incidents concerning the SPOCS framework must be reported by framework operator and MS.
- MS and framework operator must provide a contact person for Security matters.
- Develop and maintain a disaster recovery concept and conduct periodical exercises

3.2.6.2 Authentication, Authorisation & Accountability

- Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
- Assignment of privileges is based on individual personnel's job classification and function
- Requirement for an authorization form signed by management that specifies required privileges
- Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed
- Assign all users a unique ID before allowing them to access system components or data
- Implement a user life cycle management (create, change, delete of users/accounts across systems)
- Enforce a strong password policy
- Enforce idle timeouts for all administrative connections
- Prompt a banner stating that system access is only allowed for authorized users on all administrative connections.
- Use physical access control for data centres that host SPOCS components
- Separate operative staff for SPOCS components from other employees and use physical access control. If staff uses remote access, strong authentication, strong encryption, and end point security checkers must be used.
- Implement automated audit trails for all system components to reconstruct the following events:
  - All actions taken by any individual with root or administrative privileges
  - Access to all audit trails
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Initialization of the audit logs
  - Creation and deletion of system-level objects
- Record at least the following audit trail entries for all system components for each event:
  - User identification
  - Type of event
  - Date and time
  - Success or failure indication
  - Origination of event
  - Identity or name of affected
  - data, system component, or resource
- Secure audit trails so they cannot be altered. Protect audit trail files from unauthorized modifications and loss.

- Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
- Audit information must be available for the minimum of 30 days

3.2.6.3 Infrastructure

- Maintain time synchronisation to a stratum 0 clock using NTP (NTPv4 preferable, NTPv3 at least) as defined in RFC 1305
- Install and maintain a firewall and a properly segmented network for the operation and deployment of SPOCS interoperability components
- If SSL streams need to be split before the intended recipient (e.g. for load-balancing) it must be assured that the connection between the splitting component and the intended SSL-endpoint is properly secured otherwise to make interception or manipulation of the data on this connection impossible.
- Maintain an up to date documentation of network topology
- Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure
- Requirement to review firewall and router rule sets at least every six months
- Implement stateful inspection, also known as dynamic packet filtering.
- Maintain a secure environment for operators, including personal firewall on any computer or mobile device used to access the SPOCS interoperability components. Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.
- Always change vendor-supplied defaults before installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
- Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
- Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access.
- Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
- Shutdown all unused services on system components

3.2.6.4 Software

- Best practises for secure software development shall be used.
- All software used shall be subject to security testing
- Production data cannot be used for test purposes.Table 1: Operational and security requirements

4 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
    - for informative references.

NOTE: All hyperlinks included here were valid at production time. No guaranty can be provided about future availability or correctness.

4.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

- [1] ISO/IEC 27001: "Information technology - Security techniques - Information security
  management systems - Requirements".

- [2] ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management".

- [3] ISO/IEC 27005: "Information technology - Security techniques - Information security risk management".

- [4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

- [5] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

- [6] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

- [7] ETSI TS 101 862: "Qualified certificate profile".

- [8] ISO/IEC 15408 (Parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

- [9] CEN CWA 14167 (Parts 2 and 4): "Cryptographic module for CSP signing operations
with/without backup - Protection profile - CMCSOB PP/CMCSO PP".
- [10] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

4.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [i.1] ETSI TS 102 640-1: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats, Policies and Profiles; Part 1: Architecture".
- [i.2] ETSI TS 102 640-2: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Architecture, Formats, Policies and Profiles; Part 2: Data Requirements and Formats for Signed Evidence for REM".
- [i.4] ETSI TS 102 640-4: " Electronic Signatures and Infrastructures (ESI);Registered Electronic Mail (REM) Part 4: REM-MD Conformance Profiles".
- [i.4] ETSI TS 101 862 “Qualified certificate profile”
- [i.5] ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”