enisa

THE EU CYBER SECURITY AGENCY

CONFORMTY ASSESMENT OF TRUST SERVICE PROVIDERS

Technical guidelines on trust services

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use trust@functional.mailbox
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank all those who contributed to this study and reviewed it, specifically the experts and the members of national supervisory bodies, conformity assessment bodies and various trust service providers.

Legal notice
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-187-8
doi: 10.2824/066576 Catalogue number: TP-06-16-338-EN-N

Table of Contents

Executive Summary

Regulation (EU) No 910/2014[1] (hereafter the **eIDAS** Regulation), on electronic identification and trust services for electronic transactions in the internal market, provides a regulatory environment for electronic identification of natural and legal persons and for a set of electronic trust services, among them electronic signatures (Section 4), electronic seals (Section 5), electronic time stamps (Section 6), electronic registered delivery services (Section 7) and certificates for website authentication (Section 8)[2]

It is possible to use those trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

To further enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the eIDAS Regulation introduces the notions of **qualified trust service** and **qualified trust service provider** with a view to indicating requirements and obligations that ensure high-level security and a higher presumption of their legal effect.

Following the publication of the eIDAS Regulation, a set of secondary and co-regulatory acts had to be published in order to provide technical guidance on how to implement the specific requirements of the eIDAS Regulation (in the TSP part of eIDAS, the European Commission decided to publish only the mandatory ones). ENISA aimed to develop a concise set of technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies.

Every Trust Service Provider intending to start providing qualified trust services, will have to demonstrate compliance with the requirements defined by the eIDAS Regulation to the responsible Supervisory Body, through an audit or conformity assessment performed by an accredited Conformity Assessment Body.

Through this document, ENISA is supporting both Trust Service Providers and Conformity Assessment Bodies in the audit activities by presenting the auditing framework. It aims at helping Trust Service Providers fulfil the requirements defined by the eIDAS Regulation (Articles 20 and 21) as requested by Supervisory Bodies in order to grant the qualified status to a Trust Service Provider and its provided trust service(s).

The audit methodology as well as the recommendations regarding the Trust Service Providers documentation and implementation presented in this document can be used as a reference by both qualified Trust Service Providers and Conformity Assessment Bodies to support them in preparing and performing the conformity assessment as required by the eIDAS Regulation.

[1] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

1. Introduction

1.1 Purpose of the Document

The Regulation (EU) No 910/2014 (hereafter the eIDAS Regulation) repeals the Directive 1999/93/EC for electronic signatures by providing a new legal framework for "*electronic identification and trust services for electronic transactions in the internal market*". Whereas the former Directive focused on electronic signatures only, the eIDAS Regulation extends the concept of trust services to other services such as electronic seals and time stamps, registered mail and web site authentication. Under this Regulation, every Trust Service Provider intending to start providing qualified trust services, will have to demonstrate compliance with the requirements defined by the eIDAS Regulation to the responsible Supervisory Body, through an audit or conformity assessment performed by an accredited Conformity Assessment Body.

In response to the introduction of this Regulation, ENISA has decided to support both Trust Service Providers and Conformity Assessment Bodies in these audit activities by presenting the new auditing framework. This auditing framework aims at supporting Trust Service Providers willing to be granted a qualified status for the trust services they provide or in order to maintain their status by complying with all relevant requirements form the eIDAS Regulation (Articles 20 and 21), as requested by Supervisory Bodies.

In this regard, the document will describe the audit methodology followed by Conformity Assessment Bodies and will present recommendations regarding the Trust Service Providers documentation and organization which can be used as a reference to prepare and perform a conformity assessment with the respect to the eIDAS Regulation.

This auditing framework is part of the ENISA's work to develop a concise set of technical guidelines implementing the eIDAS Regulation in the non-mandatory articles, for voluntary use of all stakeholders, including Trust Service Providers, Supervisory Bodies and Conformity Assessment Bodies.[3]

The verbs "shall", "should" and "may" in this document should be used in accondance with ETSI guide[4].

1.2 Why Audit

As stated by Article 21 of the eIDAS Regulation, all Supervisory Bodies will request Trust Service Providers to demonstrate compliance with the requirements defined by the Regulation, through a conformity assessment, before notifying supervisory body of the intention to provide qualified trust services.

As stated by Article 20 of the eIDAS Regulation, once the qualified status is granted, Trust Service Providers will have to provide a new conformity assessment report to the responsible Supervisory Body, every 24 months or whenever requested by the Supervisory Body, in order to keep their qualified status.

1.3 General Concept

The diagram below provides an overview of dependencies between various stakeholders in the Trust Service Providers Assessment Scheme under the eIDAS Regulation. As seen in Figure 1, TSP sends the assessment report to the SB. The TSP then submits the assessment report to the SB within three working days after having received it (cf. Article 20 (1) of the eIDAS Regulation).

[3] https://www.enisa.europa.eu/topics/trust-services/guidelines

[4] https://portal.etsi.org/Portals/0/TBpages/edithelp/Docs/AGuideToWritingWorldClassStandards.pdf

Based on Supervisory Body decision TSP status set in Trusted List by National Authority.

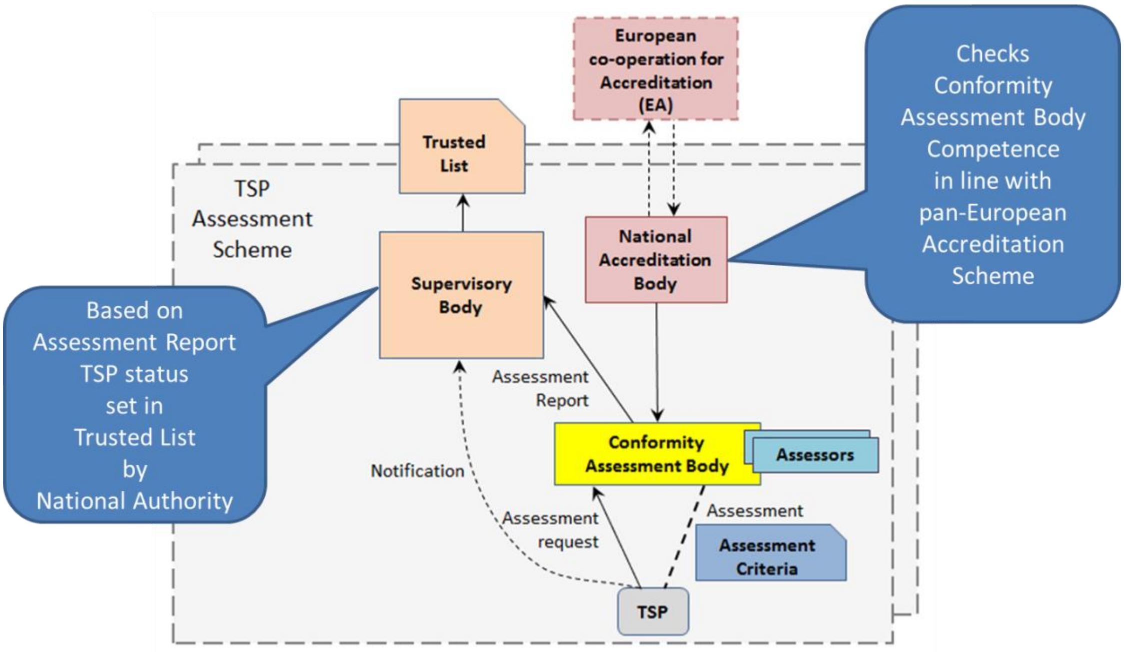
European co-operation for Accreditation (EA)
Checks Conformity Assessment Body Competence in line with pan-European Accreditation Scheme
Trusted List
TSP Assessment Scheme
National Accreditation Body
Supervisory Body
Based on Assessment Report TSP status set in Trusted List by National Authority
Assessment Report
Conformity Assessment Body
Assessors
Notification
Assessment request
Assessment
Assessment Criteria
TSP

Figure 1: Trust Service Providers Assessment Scheme

1.4 Liability of Trust Service Providers

The eIDAS Regulation states that all Trust Service Providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under that Regulation, and specifically with the Article 19.

Every national legislation on electronic signatures and on personal data protection should provide a procedure serving to demonstrate that the Trust Service Provider is applying the current national regulations, which are not affected by the transitional ones, such as the eIDAS Regulation. The intention or negligence of a qualified Trust Service Providers should be presumed unless it proves that the damage occurred without the presumed intention or negligence on its part.

The eIDAS Regulation states:

"(37) This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules."

2. Standards and Audit Methodology

2.1 Standards Related to Trust Service Providers

The tables below give an overview of the current and upcoming standards supporting Trust Service Providers in the implementation of trust services while complying with the requirements defined by the eIDAS Regulation. This section updates the previous paper released by ENISA regarding the “standardisation activities in the field of Electronic Identities and Trust Service Providers”[5].

Current standards on policy requirements (ETSI)

REFERENCE	TITLE	REPLACES
TS 119 101 V1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation	-
EN 319 401 v2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers	Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040)
EN 319 411-1 v1.1.1 (2016-02)[6]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements[7]	TS 102 042 EV & Baseline policies EN 319 411-3
EN 319 411-2 v2.1.1 (2016-02)[8]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates	TS 101 456 (& TR 102 458), EN 319 411-3
EN 319 421 v1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps	TS 102 023

[5] https://www.enisa.europa.eu/publications/standards-eidas

[6] An update is in preparation: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50522

[7] *Incorporates requirements for web site certificates with requirements previously specified in EN 319 411-3: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates*

[8] *An update is in preparation: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50523*

Current standards on certificate profiles (ETSI)

REFERENCE	TITLE	REPLACES
EN 319 412-1 v1.1.1 (2016-02)[9]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures	-
EN 319 412-2 v2.1.1 (2016-02)[10]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons	TS 102 280 & TS 101 862
EN 319 412-3 v1.1.1 (2016-02)[11]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons	-
EN 319 412-4 v1.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates	-
EN 319 412-5 v2.1.1 (2016-02)	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements	EN 319 412-5 v1.1.1 & TS 101 862
EN 319 422 v1.1.1 (2016-03)	Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles	TS 101 861

Other standards to take into consideration (ETSI, IETF, ISO)

REFERENCE	TITLE	REPLACES
TS 119 612 V2.2.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); Trusted Lists	TS 119 612 v2.1.1

[9] *An update is in preparation: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50526*
[10] *An update is in preparation: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50527*
[11] *An update is in preparation: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=50528*

IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF RFC 3280, 4325, 4630
IETF RFC 6960	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP	IETF RFC 2560, 6277, 5912
IETF RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (Trust Service Providers)	-
IETF RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	IETF RFC 2527
ISO 31000	Family of standards relating to risk management	-

Upcoming standards (ETSI)

REFERENCE	TITLE	REPLACES
EN 319 411-4	Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Requirements for trust service providers issuing code signing certificates	-
EN 319 511	Policy & security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures	TS 102 573, TR 102 572
EN 319 521	Policy & security requirements for electronic registered delivery service providers	-
EN 319 531	Policy & security requirements for registered electronic mail (REM) service providers	TS 102 640
EN 419 111-1	Protection profiles for signature creation and validation application; Part 1: Introduction to the European Norm	CWA/prEN 14170
EN 419 111-2	Protection profiles for signature creation and validation application; Part 2: Signature creation application - Core PP	CWA/prEN 14170
EN 419 111-3	Protection profiles for signature creation and validation application; Part 3: Signature creation application - Possible Extensions	CWA/prEN 14170
EN 419 111-4	Protection profiles for signature creation and validation application; Part 4: Signature verification application - Core PP	CWA/prEN 14170
EN 419 111-5	Protection profiles for signature creation and validation application; Part 5: Signature verification application - Possible Extensions	CWA/prEN 14170

2.2 Standards Related to Conformity Assessment Bodies

The table below gives an overview of current standards which support Conformity Assessment Bodies in the conformity assessment of Trust Service Providers against the requirements defined by the eIDAS Regulation. This section updates the previous paper released by ENISA regarding the "Standardisation in the field of Electronic Identities and Trust Service Providers"[12].

Current Standards (ETSI)

REFERENCE	TITLE	REPLACES
EN 319 403 V2.2.2 (2015-08)	Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers	CWA 14172 (2&8), TS 119 403
SR 003 091 V1.1.2 (2013-03)	Electronic Signatures and Infrastructures (ESI); Recommendations on Governance and Audit Regime for CAB Forum Extended Validation and Baseline Certificates	-
TR 101 564 V1.1.1 (2011-09)	Electronic Signatures and Infrastructures (ESI); Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs	-
TR 103 123 V1.1.1 (2012-11)	Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates	-
TS 103 090	Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates	-

Other standards to take into consideration (ETSI, IETF, ISO)

REFERENCE	TITLE	REPLACES
ISO/IEC 17065	Conformity assessment - Requirements for bodies certifying products, processes and services	-
ISO/IEC 17020	Conformity assessment - Requirements for the operation of various types of bodies performing inspection	-

[12] https://www.enisa.europa.eu/publications/standards-eidas

Upcoming standards (ETSI)

REFERENCE	TITLE	REPLACES
EN 419 103	Conformity assessment for signature creation & validation (applications & procedures)	-

2.3 Audit Methodology

As required by the eIDAS Regulation, a conformity assessment must be performed by an accredited Conformity Assessment Body either when a Trust Service Provider is intending to start providing qualified trust services (Article 21) or to verify that a qualified Trust Service Providers and the qualified trust services they provider still fulfil the requirements laid down in the Regulation (Article 20). In the second case, this conformity assessment must be performed at least every 2 years but can also be requested at any time by the Supervisory Body (Article 17).

This section presents the general approach for Conformity Assessment Bodies to assess the conformity of Trust Service Providers and the trust service(s) they provide as recommended by the standard *ETSI EN 319 403 Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers*[13]. This standard presents, for each step of the audit, all the general requirements for evaluating Trust Service Providers against the requirements set out in the eIDAS Regulation. It includes the specificities of the type of trust service to be assessed, various aspects of the Trust Service Providers activities to be covered and relevant standards (e.g. ETSI) as well as other potential regulatory requirements to be taken into account.

The audit process will be split into 3 parts:

- **Stage 0:** General preparation **-** to agree on the terms of the audit (time, location, scope, etc.).
- **Stage 1:** Documentation review **-** to review the documentation regarding the Trust Service Providers and trust services provided.
- **Stage 2:** On-site audit - to validate the preliminary findings and complete the audit against the defined assessment criteria.

At the end of the process, a conformity assessment report containing all the results of the audit will be issued by the Conformity Assessment Body to the Trust Service Providers. The final decision regarding the qualification of the Trust Service Providers and its trust services will be taken by the responsible Supervisory Body based on this report and any additional information requested from TSP which was necessary to verify compliance with the requirements laid down in eIDAS regulation

2.3.1 Stage 0: General Preparation

Before starting the audit, the Conformity Assessment Body will perform a set of preparation activities in order to define and agree with the Trust Service Provider on the plan and scope of the audit. This initial stage will allow to set the timing of the audit as well as the exact locations where the stages will take place.

Next to that, the Conformity Assessment Body will establish the initial list of up-to-date documents, regarding the Trust Service Provider and the trust services it provides, which are required to perform the conformity assessment.

[13] http://www.etsi.org/deliver/etsi_en/319400_319499/319403/02.02.02_60/en_319403v020202p.pdf

The set of documentation typically includes:

- Trust Service Provider related details (trust services, locations, sizes, functions);
- policies and practices (CP/CPS);
- provision and operation of trust services;
- technical documentation (IT network infrastructure regarding trust services);
- terms and conditions;
- contractual documents with third parties;
- evidences for secure and conformant operations like logs and protocols.
- termination Plan

2.3.2 Stage 1: Documentation Review

During the first stage of the audit, the Conformity Assessment Body will develop its understanding of the structure and extent of trust services provided by the Trust Service Provider, before defining an appropriate planning for the stage 2 of the audit.

If required by the audit activities, the Conformity Assessment Body can, at any time, request additional information to the Trust Service Provider (e.g. records, design of trust services, etc.).

Besides the review of documentation, the Conformity Assessment Body activities will also include the verification of other elements such as:

- records regarding legal entity;
- contractual arrangements;
- arrangements of liabilities;
- other audit reports and certifications.

Incident management, for example, takes an important place in the eIDAS Regulation and all activities regarding the reporting of security breach or loss of integrity should be taken into account seriously by all Trust Service Providers. In this regard, ENISA is working with a group of experts for the purpose of developing technical guidelines regarding the reporting of incidents by Supervisory Bodies.[14]

At the end of stage 1 the Trust Service Provider will be provided with a first finding report by the Conformity Assessment Body. This report contains the results of the first stage of the audit and highlights the areas of concerns along with recommendations. Although minor issues can remain open and treated during the next stage of the audit, most of the identified issues need to be resolved before starting the stage 2.

Next to this report, the Conformity Assessment Body will also share the planning of stage 2 with the Trust Service Provider and request additional information or records if required for the second stage.

2.3.3 Stage 2: On-site Audit

Once all activities of stage 1 are completed and main areas of concerns resolved by the Trust Service Provider, stage 2 of the audit can be started. This stage takes place on site, at the Trust Service Provider, and has the purpose of demonstrating whether the Trust Service Provider and the trust services it provides comply with its own policies and procedures as well as the defined assessment criteria (based on the eIDAS

[14] https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting

requirements, relevant standards, etc.). All evidences, records and logs of every action should be kept safe and recorded to be handed over to the Conformity Assessment Body.

For this, the Conformity Assessment Body will collect evidences regarding the Trust Service Provider and its trust services:

- implementation of trust service requirements;
- trust service related processes and procedures;
- trust service related products (trustworthy systems);
- information security measures for trust services;
- physical security of relevant Trust Service Providers sites.

In order to complete this stage 2 audit, a conformity assessment report providing all results and other relevant details of the assessment will be issued to the Trust Service Provider.

2.3.4 Conformity Assessment Report

After successful completion of the audit (i.e. stages 1 and 2), the Conformity Assessment Body will issue a conformity assessment report. This detailed report contains all results of the assessment performed and is provided to the audited Trust Service Provider. The Trust Service Provider must in turn provide this report to the responsible Supervisory Body within 3 working days. Only after a full review of the conformity assessment report and any additional information requested from TSP which was necessary to verify compliance with the requirements laid down in eIDAS regulation will the Supervisory Body decide whether the Trust Service Provider and the trust services it provides comply with the requirements set out it the RegulationMaximum 3 months after the submission of the conformity assessment report, the Trust Service Provider will be notified with the decision from the Supervisory Body. If positive, the Trust Service Provider and the audited trust services will be granted the “qualified” status and will be added to the national trusted list by the responsible body, if not already within. In case a qualified Trust Service Provider and its qualified trust services do not meet the requirements set out in the Regulation, the Supervisory Body will not grant qualified status (in case of a new TSP/TS) or will withdraw the qualified status and inform the body responsible for the national trusted list about its decision.

3. Trust Service Providers’ Documentation

As part of its audit activities, the Conformity Assessment Body will request specific documentation supporting the implementation of the Trust Service Providers organization. This documentation will be reviewed at the first stage of the audit and will serve as a basis for the audit on-site performed during the stage 2. In this sense, it is essential for Trust Service Providers to make sure the appropriate documents such as plans, policies and procedures are defined and continuously updated following the Trust Service Providers changes.

The purpose of this section is to present an overview of the typical documentation to be maintained by Trust Services Providers following recognized frameworks and standards such as IETF, NIST or ETSI. Related information and more specifically the policy and security requirements as well as technical specifications for Trust Service Providers can be found in the document “Recommendations for TSPs based on Standards ” created by ENISA.[15]

3.1 Plans

Plans are high-level statements that aim at providing a clear understanding of the long-term objectives defined by the Trust Service Providers throughout the organization, and are periodically reviewed and updated by the management. Trust Service Providers should create plans to cover the various aspects of the organization such as the security, management of systems, business continuity, management of incidents, etc.

3.1.1 Infrastructure Management Plan

In order to respond to the continuous system evolution, Trust Service Providers should define a plan to manage and monitor the entire infrastructure, including the following components:

- the servers (CPU, storage, memory, etc.);
- the databases (table spaces, data files, file systems);
- the networking devices;
- the security controls (firewalls, IPSs).

3.1.2 Organization Structure

An organization exists as a system of coordinated activities accomplishing its defined goals and objectives according to the defined strategy. The structure of a Trust Service Provider is managed in a hierarchical manner, where well defined and repetitive tasks are set at the lower level and more flexibility to perform higher priority tasks are set at the higher level.

For this purpose, clear roles and responsibilities must be defined and assigned to personnel, based on their place in the hierarchy, in order to perform their tasks efficiently. It should also include recommendations enforcing security measures as well as methods to maintain the personnel discipline.

3.1.3 Security Plan

A security plan supports Trust Service Providers in ensuring the continuous protection of their IT resources by providing a clear overview of the security requirements and describing the management, operational as

[15] https://www.enisa.europa.eu/topics/trust-services/guidelines

well as technical controls in place. The plan should also address the roles and responsibilities regarding the access to the resources and the associated authorizations.

For the creation of security plan, Trust Service Providers should follow existing standards such as ISO/IEC 27001[16] and make sure it is aligned with other plans such as the risk management plan, business continuity plan or incident management plan.

3.1.4 Communication Plan

In order to ensure an efficient exchange of all the required information internally but also outside the organization (e.g. with customers), Trust Service Providers must have a dedicated communication plan in place.

This plan presents the type of information published and the way this is done, but also defines the target audience as well as potential impacts on the Trust Service Providers and provided trust services.

Based on the target audience and the type of information to be communicated, Trust Service Providers may categorize communication as follows:

- internal communication (e.g. to employees);
- business communication (e.g. to customers);
- emergency communication;
- media communication;
- shareholders communication.

Internal communication will follow procedures that differ from the ones used for external communications (e.g. announcement of a new product).

3.1.5 Risk Management Plan

As the networked world continues to shape and impact every aspect of our lives, threats to the global industry continue in parallel.

For this purpose, Trust Service Providers must have an appropriate risk management plan in place to support the identification and evaluation of emerging risks and the implementation of appropriate controls to avoid them.

Technical guidelines regarding the conduction of a risk assessment on Trust Service Providers as part of the eIDAS Regulation can be found in the document "Recommendations for TSPs based on Standards " created by ENISA. [17]

3.1.6 Business Continuity Plan

In order to ensure the preservation of its business (e.g. trust services) during and after a disaster, Trust Service Providers should have a well-defined business continuity plan (including disaster recovery plan and contingency plan) as part of its response planning.

[16] http://www.iso.org/iso/iso27001
[17] https://www.enisa.europa.eu/topics/trust-services/guidelines

This plan aims at describing all the arrangements foreseen by the Trust Service Providers, including processes and procedures, to recover as quickly as possible from any kind of major disruption regarding its network or its systems and continue to provide its services.

The business continuity plan should be maintained, tested and be subject of training. As part of its implementation, this plan will require the creation of two other plans: a disaster recovery plan and a contingency plan.

3.1.6.1 Disaster Recovery Plan (DRP)

The disaster recovery plan defines the technical and functional requirements to protect the IT infrastructure of Trust Service Providers and restore its operability following a disaster.

Analysis and availability of critical recovery resources is important in order to develop the ongoing recovery cost estimates. There should be specific recovery strategies defined for IT as well as business processes.

Some requirements to consider regarding the IT infrastructure include:

- systems hardware resources;
- systems data storage requirements;
- unique (i.e. nonstandard) hardware resources;
- distributed systems (e.g. workstations, extranet, intranet, etc.).

3.1.6.2 Contingency Plan

A contingency plan defines all the interim measures, such as the relocation of systems to a back-up site, which are in place to help Trust Service Providers recover from a disaster and ensure the continuation of its services. This plan can include several phases including detection, notification, evaluation and resolution, which must be described and checked.

3.1.7 Incident Management Plan

Trust Service Providers should have a plan to manage incidents impacting their infrastructure and that can affect the normal operation of the services provided., This plan should include specific information such as the incident category as well as the measures to mitigate the impact and prevent further damage to the Trust Service Providers operations.

It is recommended that Trust Service Providers align this incident management plan with other plans such as the business continuation plan as part of the response operations.

3.1.8 Training Plan

Given the complexity of Trust Service Providers environment, all personnel (e.g. employees, subcontractors) should be educated and receive guidance for the most important aspects of Trust Service Providers operations. For this purpose, the Trust Service Providers should define a clear plan describing the type of trainings required and how they can be given according to the target audience.

Many topics that should be covered by the training plan, including:

- corporate policies;
- regulatory compliance;
- business continuity and disaster recovery;
- risk management;

- physical and logical infrastructure.

Moreover, the training plan should inform personnel about their roles and responsibilities as well as the surrounding expectations.

3.1.9 Legal Enforcement Plan

TPSs should have a clear plan to address the major legal obligations at national and international level, which can affect the services provided.

Besides the eIDAS Regulation, Trust Service Providers may be subject to other applicable laws such as:

- national laws related to electronic signatures;
- personal data protection laws;
- contract laws.

3.1.10 Access Control Plan

Trust Service Providers should have a clear and agreed plan regarding control of personnel access to the IT resources, as either logical (e.g. systems, databases) or physical (e.g. facilities), in order to prevent undesired access.

This plan should describe the requirements (i.e. type of users, resources to access, operations to perform, etc.) and controls in place to restrict access and therefore ensure the protection of the resources.

3.1.11 Termination Plan

Trust Service Providers providing qualified trust services should have an up-to-date termination plan[18] to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4).

Thus, aiming to ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.

3.2 Policies

Policies are principles, rules or guidelines established and adopted by Trust Service Providers to influence or determine the way of proceeding in specific cases or areas.

It should be noted that any creation or update to existing policies should be reviewed and receive the approval from the responsible Internal Governance Body before its publication. Trust Service Providers should define a similar body which is responsible for the control and the maintenance of all the policies and practices (e.g. CP/CPS) within the organization, as well as the review of audit results to check policy compliance.

3.2.1 Security Policy

The security policy is the main policy in place regarding the objectives of an organization to protect its assets. This policy defines the main rules set by the organization and to be followed in order to ensure the security of all IT resources, facilities but also personnel within the organization.

[18] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

Trust Service Providers should write a security policy covering specific areas such as:

- Risk Management;
- Disaster Recovery;
- User Responsibilities;
- Internet and E-mail Policies;
- Password Policies.

3.2.2 Access Control Policy

The access control policy defines the rules set by an organization regarding the access to its IT resources by all entities within or outside the organization (e.g. employees, customers).

Trust Service Providers should develop an access control policy to clearly set the requirements regarding the identification, authentication, authorization and monitoring of who or what is accessing specific resources in order to protect the company from threats and vulnerabilities, related to undesired access to the Trust Service Providers assets.

3.2.3 Certificate Policy and Certification Practice Statement

The X.509 standard defines a Certificate Policy (CP) as "*a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements*".

In general, as mentioned above, there are two major categories of CPs:

- Focused on indication applicability of a certificate to a particular community (e.g. geographical region, specific market or finance, assurance, etc.).
- Focused on indication applicability of a certificate to a class of application with common security requirements (e.g. different level of security and level of assurance).

The CP can be represented in a certificate by a unique number called an Object Identifier (OID) which can be registered and assigned to a particular organization.

The DSG defines a Certification Practice Statement (CPS) as "*a statement of the practices which a certification authority employs in issuing certificates*"[19].

In other words, the CPS establishes the practices used by a CA regarding the management of the certificates lifecycle (e.g. certificate issuance, revocation, re-key, etc.).

While the CP defines the requirements and appropriate usage for the certificate types issued by the PKI, the CPS states the PKI actors, their roles and duties, and describes the practice employed by the CA following best practices and requirements defined in the CP.

The RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework"*[20] provides some guidance and the recommended structure for the creation of a CP and/or CPS:

[19] American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996.
[20] https://www.ietf.org/rfc/rfc3647.txt

1. Introduction
2. Publication and Repository Responsibilities
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance Audit and Other Assessments
9. Other Business and Legal Matters

Trust Service Providers willing to issue qualified certificates can follow the ETSI EN 319 411-2 *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"*[21]. This standard supports Trust Service Providers in the writing of their CP and/or CPS by providing the general policy and security requirements that meet the requirements set out in the eIDAS Regulation, including Articles 19, 24, 28, 38 and 45.

The CP and CPS constitute both a basis for most of audits, accreditations, and other assessments of a Trust Service Providers.

3.2.4 Archive Policy

The archive policy is an internal document maintained by Trust Service Providers to define the rules regarding the archival of critical information, due to either business or legal requirements.

This policy sets the rules regarding the archival process, specific to the type of data to be archived. It includes information such as the archiving criteria, mechanism and storage used, retention period as well as the people authorized to perform the archive.

3.3 Procedures

Procedures are step-by-step instructions to be followed in order to perform specifics tasks. They support the implementation of the plans and policies defined by the Trust Service Providers in a consistent and regular basis by providing clarity and a common understanding of the operations. Usually, procedures come along with well-defined roles and responsibilities.

In order to reduce the risks that important steps, communication and required deliverables are left out, procedures should be best developed with input of interfacing areas. Moreover the associated documentation should be consistent in order to give the ability to improve and facilitate the review of the procedures in place.

3.3.1 Operations Security

Operations security procedures aim at supporting Trust Service Providers in ensuring the security of their operations by protecting and controlling their information assets.

Moreover, these procedures should encompass all the required tasks in order to ensure the availability of all IT resources.

Operations security procedures can be divided into different areas such as:

[21] http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf

- roles and responsibilities for trusted personnel operators (e.g. system/security admins, auditors);
- resources protection (e.g. facilities, hardware, software);
- continuity of operations (e.g. business continuity and disaster recovery);
- change control management.

3.3.2 Change Control Management

Trust Service Providers systems require frequent changes, due to software packages added, removed or modified, or because of the introduction of new hardware.

This rapid advancement of technology requires proper change management control procedures in order to perform maintenance activities in a controlled way and ensure the integrity of the necessary systems.

Trust Service Providers should indicate the scope of the affecting system(s) (e.g. on test, production) and of the kind of modification (e.g. permanent changes, temporary changes, emergency changes) and the procedure associated to it. All these requirements should be defined accordingly and a responsible person should be designated for every asset. These procedures should have a workflow including at least:

- identification of the change (e.g. affected services);
- technical evaluation and risks associated to the change;
- approval of the change;
- information of the change (e.g. according to the communication policy);
- execution of the change;
- new testing to validate the change.

For recovery and integrity purposes, a detailed inventory of the hardware and software is necessary.

3.3.3 Risk Assessment

Risk assessment procedures should provide all the requirements for assessing risks with regards to Trust Service Providers operations. These procedures should support personnel in identifying, understanding and evaluating the risks in order to take the appropriate actions to tackle them using the appropriate measures. In order to keep track of actions taken and leave room for improvement, all identified risks as well as relevant associated information should be recorded for further analysis.

For information on the risk analysis procedure, please consult ENISA guidelines published in 2013[22].

3.3.4 Network Security

Network security includes the structures, transport methods and formats, as well as all security measures in place to ensure integrity, availability and confidentiality of all Trust Service Providers' data transferred over private and public networks.

Since any loss of network connectivity, internally or externally, may have disastrous consequences, ensuring network security is one of the main keys for Trust Service Providers.

Procedures associated to network security should consist of a list of specific actions to be executed at different levels, including:

- physical and logical network protection (e.g. network segmentation, configuration of network security devices, security patches, permissions granting);

[22] https://www.enisa.europa.eu/activities/identity-and-trust/trust-services/guidelines-tsp

- trusted roles and system accounts (e.g. roles and responsibilities, access control);
- logs, monitoring and alerts (e.g. network infrastructure monitoring, alerts configuration, logging records, vulnerabilities detection).

3.3.5 Incident Response

Incident response procedures define all the precise steps to be followed in order to address and manage the consequences of an incident (e.g. security breach) and mitigate its impact, according to the defined plan. The procedures should indicate all the details required to appropriately handle a specific type of incident, including:

- level of importance;
- response time;
- responsible people;
- communication needs.

3.4 Evidence management

Evidence is collected with the purpose of providing details regarding an event and demonstrating the effectiveness of associated procedures. Measurement of this information provides the ability to improve the procedures.

3.4.1 Evidence Documentation

For every defined plans, policies and procedures, Trust Service Providers should obtain evidence that the related documents are consistently followed up. For this purpose, tools can support the Trust Service Providers in the execution of specific tasks, and provide efficient management of all analogous information.

For example, there are tools supporting the execution of risk analysis or the management of Trust Service Providers assets (i.e. their location, owners, characteristics, etc.).

3.4.2 Testing

All tests performed within the Trust Service Providers infrastructure should be documented along with all associated information and the required level of detail (e.g. test type, plan testing, quality status, etc.).

3.4.3 Agreements and Contracts

All contracts and agreements such as NDAs, SLAs and confidentiality agreements, between Trust Service Providers and their employees, customers or other third parties should be maintained and kept in a safe place in order to protect the company in case of dispute.

3.4.4 Evaluation Reports

In order to ensure the effectiveness and proper functioning of the resources, evaluation of all hardware and software in place at the Trust Service Providers should be performed on a regular basis, generating evaluation reports as well as evidence that should be recorded. Evaluation reports can also be generated following other kinds of activities such as personnel trainings (e.g. tests) or audits (e.g. findings).

3.4.5 Event Logs

Logging events can help the Trust Service Providers track issues and find the root causes in case of incidents such as system failures or security breaches. For this purpose, all the logs generated by a system with regards to specific events should be recorded and stored accordingly by the Trust Service Providers.

3.4.6 Regulatory Compliance

In order to show compliance with the eIDAS Regulation as well as, where applicable, other national or international laws, all relevant evidence that can be used as a proof of compliance should be recorded and stored by the Trust Service Providers.

4. Trust Service Providers Organization

4.1 Trust Service Providers Services

This section describes the various component services related to the certification services. It focuses mainly on certification services because they form the foundation of all trust services under the eIDAS Regulation, such as electronic signatures, seals or time stamps. Any Trust Service Provider willing to provide qualified trust services will first have to make sure its certification service or its third-party service provider fulfils all the requirements set out in the eIDAS Regulation regarding the issuance of qualified certificates for the defined purpose. The subdivision of services is only for the purposes of clarification and does not place any restrictions on the implementation of the Trust Service Providers services.

4.1.1 Registration Service

The registration service verifies the identity and if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service (section 4.1.2).

This service is often provisioned by a Registration Authority (RA), which has formal agreement with the Certification Authority (CA) to identify and authenticate the certificate subjects, verify the documentation accrediting the circumstances appearing in the certificates and validate the requests to issue, revoke or renew certificates.

The RA should assume the following obligations:

- Validating the identity and other personal details of the subject of the certificates or information relevant for the purpose of the certificates in accordance with the associated procedures.
- Maintaining all information and documentation concerning certificates, and managing their issuance, renewal, revocation and reactivation.
- Notifying the CA of certificate revocation requests with due diligence and in a fast and reliable manner.
- Informing the CA of all issuance, renewal and reactivation requests, and any other aspects of certificate management.
- Validating with due diligence the circumstances for revocation that might affect the certificate validity.
- Performing its certificate management operations in compliance with the procedures established by the Trust Service Providers and current legislation.
- Where applicable, making available to the subject the technical procedures for signature creation data (i.e. the private key) and electronic signature verification (i.e. the public key).

The process associated to the proper identification of the subscriber is the responsibility of the Trust Service Providers, and should be performed prior to the issuance of the certificate.

The certificate will only be issued if this process is completed successfully, otherwise the RA will refuse the request and inform the applicant of the reasons.

4.1.2 Certificate Generation Service

Subscriber certificates can be issued either by means of a cryptographic device or a software mechanism.

4.1.2.1 Cryptographic Device

The typical issuance procedure for certificates issued using a cryptographic device is the following:

1. The RA verifies the validity of the documentation submitted by the applicant.
2. Following the applicant authentication, the RA requests a certificate from the CA.
3. The CA issues the certificate to the RA following the established procedures.
4. The RA securely downloads the certificate on the signature creation device.

4.1.2.2 Software Mechanism

The issuance procedure for certificates issued using a software mechanism is the following:

1. The RA verifies the validity of the documentation submitted by the applicant.
2. Together with the application form, the applicant generates a key pair giving the public key.
3. After receiving the documentation and the public key, the CA issues the certificate.
4. The private key and the certificate are stored on the cryptographic device or on the computer of the subscriber.

4.1.3 Subject Device Provision Service

The subject device provision service is an optional service which aims at preparing, and providing or making available secure cryptographic devices, or other secure devices, to subjects.

4.1.4 Dissemination Service

The purpose of the dissemination service is to disseminate the certificates to subjects, and in case of subject consents, make them available to relying parties. This service also makes available the Trust Service Providers terms and conditions as well as any published policy and practice information (e.g. CP/CPS) to subscribers and relying parties.

Depending on the method used to issue the certificate, the associated private key will be delivered to the entities in a different way:

- If the certificate is issued on a cryptographic hardware device (section 4.1.2.1), the private key is delivered on the cryptographic device.
- If the certificate is issued on a software mechanism (section 4.1.2.2), the private key is generated by the server and does not need to be delivered.

4.1.5 Revocation Management Service

The revocation management service processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

Various reasons can lead to the revocation of certificates, which can vary according to the nature of the certificate (i.e. subscriber or CA certificate).

Trust Service Providers must provide a process for subscribers to request the revocation of their certificate, which should be described in the available CP/CPS. The qualified Trust Service Providers shall maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

In regards to private key compromise, certificate misuse and other types of fraud or inappropriate conduct, the Trust Service Providers must provide third parties with clear instructions for reporting through readily accessible online means.

For instance, some reasons to request the revocation of a certificate may the following:

- loss or compromise of the private key;

- legal or administrative order;
- subscriber employment termination.

4.1.6 Revocation Status Service

The certification revocation status service provides certificate status information to relying parties, either based upon revocation lists or using an online service providing status information on an individual basis.

The two common schemes for certificate status validation are: Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP).

As required by the eIDAS Regulation (Article 24), every request for the revocation of a qualified certificate must be handled by the Trust Service Providers and the new status published at maximum 24 hours after the receipt. The revocation becomes effective immediately after its publication.

4.1.6.1 Certificate Revocation List (CRL)

A CRL is a time-stamped list containing all the revoked certificates which is signed by the issuing CA (or another CRL issuer) and made available through a public repository.

There are some recommendations that a CRL for end entity certificates should be issued at least every 24 hours or when a revocation occurs, and should be valid for 10 days.

All recommended specifications regarding the management of CRLs can be found in the RFC 5280.

4.1.6.2 Online Certificate Service Protocol (OCSP)

Trust Service Providers may also provide third parties with a real-time online service based on OCSP, which allows to immediately verify the status of a certificate. This service should be available 24 hours a day, 7 days a week. OCSP responses are signed either by the CA who issued the certificate or the OCSP responder.

All recommended specifications regarding the protocol OCSP can be found in the RFC 6960.

4.2 Trust Service Provider Infrastructure

As part of the requirements form the eIDAS Regulation, Trust Service Providers must address physical and logical security related to their infrastructure using all appropriate countermeasures as well as defensive and recovery strategies. Further information regarding the infrastructure of Trust Service Providers and trust services (including entities, assets and processes to be protected) can be found within the other technical guideline documents developed by ENISA[23].

4.3 Personnel Security

Trust Service Providers should implement procedures for personnel regarding security issues and how to proceed accordingly. Specific procedures regarding "trusted roles"[24] should be clearly defined by Trust Service Providers, along with the associated tasks to be performed.

In order to make sure that people with trusted roles perform their corresponding duties properly, the following considerations should be addressed by Trust Service Providers:

[23] https://www.enisa.europa.eu/topics/trust-services/guidelines

[24] A trusted role is defined as a set of responsibilities assigned to a person, and that can lead to security problems if not performed satisfactorily, either accidentally or maliciously.

- The technology is designed and configured in order to prevent errors and improper conduct.
- The duties are distributed among several individuals so that any action must be approved by at least two people.

The Trust Service Providers should make available a full inventory of all the roles carried out in the organization, along with associated duties and responsibilities. Each of these roles should come with a clear definition as well as a set of documented procedures.

4.3.1 Personnel controls

Trust Service Providers should implement several controls regarding the personnel requirements and needs:

- Background, qualification and experience (i.e. personnel should have the required experience and qualification to perform their job);
- Training (i.e. provide personnel with the required trainings and maintain records);
- Retraining (i.e. new training plan following any significant change to CA operations);
- Sanction for unauthorized actions (i.e. internal disciplinary regime defining the sanction against personnel);
- Contracting personnel (i.e. maintenance of specific policies regarding contracting personnel);
- Documentation (i.e. provide all personnel with required Trust Service Providers documentation such as CP/CPS, operations manuals, etc.).

5. Conclusions

This document provided an overview of the auditing framework for Trust Service Providers as part of the eIDAS Regulation and articles 17, 20 and 21 in particular. It discussed the available standards and methodology used to perform the conformity assessment as well as the relevant documentation and recommended implementation for Trust Service Providers organizations.

All information presented in this document can be followed as reference by both Trust Service Providers and Conformity Assessment Bodies for the purpose of preparing and performing the conformity assessment, as required by the eIDAS Regulation, in the best possible conditions. It presented the measures that can be taken at organizational level, drawing to norms and standards for technical details. Besides the eIDAS Regulation, this framework can also serve as baseline for other kinds of Trust Service Providers assessments or audits.

Main requirements and examples were provided in the context of qualified Trust Service Providers providing service for to the issuance of qualified certificates, however these also apply to other Trust Service Providers and trust services as defined in the Regulation.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-06-16-338-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-187-8
DOI: 10.2824/066576