CHANGES / SPREMEMBE

Revision Revizija	Opis spremembe	Change description	Date Datum
05	V točki 5 alineja (e) dodan elektronski naslov za obveščanje o spremembah (eidaschange@si.bureauveritas.com) V točko 5 odsek "(Začetna / Certifikacijska presoja) " je dodano pojasnilo vloge tehničnega eksperta. V točki 5 odsek "(Neskladnosti)" je usklajena zahteva kot "Odobritev certificiranja z odprtimi neskladnostmi pri ni dovoljena.". Ukinjena je delitev neskladnosti na manjše in večje in se v celotnem področju SPA 17 uporabljajo samo "Neskladnosti". Dodana je zahteva za preverjanje uspešnosti uvedenih ukrepov. V točki 5 odsek "(Reklamacije in prizivi)" je spremenjen postopek za reklamacije in prizive.	In chapter 5 paragraph (e) e-mail address for notification of changes (eidaschange@si.bureauveritas.com) is added An explanation of the role of the technical expert is added in chapter 5 of the section "(Initial / Certification Assessment)". In chapter 5, section "(Non - conformity)", the harmonized requirement is as "Approval of certification with open non - conformity is not allowed.". The division of non-conformity into smaller and larger ones has been abolished and only "Non-conformity" are used in the entire area of SPA 17. A requirement has been added to verify the effectiveness of the actions introduced. In chapter 5 of the section "Complaints and appeals ("), the procedure for complaints and appeals has been changed.	27.06.2018
06	Razširitev obsega akreditacije	Extension of the scope of accreditation	06.06.2019
07	Vključene zahteve o zagotavljanju aktivnosti certificiranja v izvršljivi obliki; Dodane verzije standardov.	Included requirements for providing certification activities in an enforceable form; Added versions of standards.	16.07.2019
08	Izdelana je dvojezična verzija SVN / EN. V točki 5 alineja (e) spremenjen elektronski naslov za obveščanje o spremembah (eidas-slovenia@bureauveritas.com). V točki 7 je spremenjen naslov za oddajo pritožb in apelov (https://www.bureauveritas.si/mnenje-strank-pritozbe-prizivi). Zamenjan izraz "Inšpektor" s predstavnik "NOD" in "MJU" z "NOD".	A bilingual version of SVN / EN has been produced. In chapter 5 paragraph (e) changed the e-mail address for notification of changes (eidas-slovenia@bureauveritas.com). In chapter 7 the address for complaints and appeals (https://www.bureauveritas.si/mnenje-strank-pritozbe-prizivi) is changed. Replaced the term "Inspector" with a "representative of the NOD" and "MJU" with a "NOD".	25.05.2020

CONTENT / KAZALO

1. NAMEN IN PODROČJE UPORABE

Ta dokument opredeljuje postopke, s katerimi družba Bureau Veritas d.o.o. (v nadaljnjem besedilu: BV) ureja formalne postopke za certificiranje kvalificiranih storitev zaupanja v skladu z uredbo (EU) št. 910/2014 »eIDAS«.

2. TERMINOLOGIJA IN DEFINICIJE

V tem dokumentu in pripadajoči dokumentaciji, ki je v uporabi v procesu certificiranja kvalificiranih storitev zaupanja v skladu z uredbo (EU) št. 910/2014 »eIDAS«, se uporabljajo naslednje opredelitve pojmov:

- „**elektronska identifikacija**“ pomeni postopek uporabe identifikacijskih podatkov osebe v elektronski obliki, ki enolično predstavljajo bodisi fizično ali pravno osebo bodisi fizično osebo, ki zastopa pravno osebo;
- „**sredstvo elektronske identifikacije**“ pomeni materialno in/ali nematerialno enoto, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletnih storitvah;
- „**identifikacijski podatki osebe**“ pomeni niz podatkov, ki omogočajo, da se določi identiteta fizične ali pravne osebe ali fizične osebe, ki zastopa pravno osebo;
- „**shema elektronske identifikacije**“ pomeni sistem za elektronsko identifikacijo, v okviru katerega se fizični ali pravni osebi ali fizični osebi, ki zastopa pravno osebo, izdajo sredstva elektronske identifikacije;
- „**avtentikacija**“ pomeni elektronski postopek, ki omogoča potrditev elektronske identifikacije fizične ali pravne osebe ali izvora in celovitosti podatkov v elektronski obliki;
- „**zanašajoča se stranka**“ pomeni fizično ali pravno osebo, ki se zanaša na elektronsko identifikacijo ali storitev zaupanja;
- „**organ javnega sektorja**“ pomeni državni, regionalni ali lokalni organ, osebo javnega prava ali združenje, ki jo/ga ustanovi eden ali več takšnih organov ali ena ali več takšnih oseb javnega prava, ali zasebni subjekt, ki ga je vsaj eden od teh organov, oseb ali združenj pooblastil za zagotavljanje javnih storitev, kadar deluje v okviru tega pooblastila;
- „**oseba javnega prava**“, pomeni osebo, opredeljeno v točki 4 člena 2(1) Direktive 2014/24/EU Evropskega parlamenta in Sveta (15);
- „**podpisnik**“ pomeni fizično osebo, ki ustvari elektronski podpis;
- „**elektronski podpis**“ pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani in jih podpisnik uporablja za podpisovanje;

1. PURPOSE AND AREA OF USE

This document defines the procedures with which Bureau Veritas d.o.o. (hereinafter: the BV) regulates its formal processes for certifying qualified trust services in accordance with Regulation (EU) No. 910/2014 "eIDAS".

2. TERMINOLOGY AND DEFINITIONS

In this document and the corresponding documentation, which is used in the process of certifying qualified trust services in accordance with Regulation (EU) No. 910/2014 "eIDAS", the following definitions of terms are applied:

- "**electronic identification**" means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- "**electronic identification means**" means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- "**person identification data**" means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- "**electronic identification scheme**" means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
- "**authentication**" means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
- "**relying party**" means a natural or legal person that relies upon an electronic identification or a trust service;
- "**public sector body**" means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
- "**body governed by public law**" means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15);
- "**signatory**" means a natural person who creates an electronic signature;
- "**electronic signature**" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

– „**napredni elektronski podpis**“ pomeni elektronski podpis, ki izpolnjuje zahteve iz člena 26;	– "**advanced electronic signature**" means an electronic signature which meets the requirements set out in Article 26;
– „**kvalificirani elektronski podpis**“ pomeni napredni elektronski podpis, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega podpisa in temelji na kvalificiranem potrdilu za elektronske podpise;	– "**qualified electronic signature**" means an advanced electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures;
– „**podatki za ustvarjanje elektronskega podpisa**“ pomeni enolične podatke, ki jih podpisnik uporablja za ustvarjanje elektronskega podpisa;	– "**electronic signature creation data**" means unique data which is used by the signatory to create an electronic signature;
– „**potrdilo za elektronski podpis**“ pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe;	– "**certificate for electronic signature**" means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
– „**kvalificirano potrdilo za elektronski podpis**“ pomeni potrdilo za elektronske podpise, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge I;	– "**qualified certificate for electronic signature**" means a certificate for electronic signatures that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;
– „**storitev zaupanja**“ pomeni elektronsko storitev, ki se praviloma opravlja za plačilo in vključuje:	– "**trust service**" means an electronic service normally provided for remuneration which consists of:
(a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali	(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
(b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali	(b) the creation, verification and validation of certificates for website authentication; or
(c) hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami;	(c) the preservation of electronic signatures, seals or certificates related to those services;
– „**kvalificirana storitev zaupanja**“ pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve iz te uredbe;	– "**qualified trust service**" means a trust service that meets the applicable requirements laid down in this Regulation;
– „**organ za ugotavljanje skladnosti**“ pomeni organ, opredeljen v točki 13 člena 2 Uredbe (ES) št. 765/2008, ki je akreditiran v skladu z navedeno uredbo in je pristojen za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja, ki jih ta zagotavlja;	– "**conformity assessment body**" means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
– „**ponudnik storitev zaupanja**“ pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja;	– "**trust service provider**" means a natural or a legal person who provides one or more trust services as a provider of either qualified or non-qualified trust services;
– „**ponudnik kvalificiranih storitev zaupanja**“ pomeni ponudnika storitev zaupanja, ki zagotavlja eno ali več kvalificiranih storitev zaupanja in mu nadzorni organ dodeli kvalificirani status;	– "**qualified trust service provider**" means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
– „**izdelek**“ pomeni strojno ali programsko opremo ali ustrezne sestavne dele strojne ali programske opreme, katerih uporaba je namenjena zagotavljanju storitev zaupanja;	– "**product**" means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
– „**naprava za ustvarjanje elektronskega podpisa**“ pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega podpisa;	– "**electronic signature creation device**" means configured software or hardware used to create an electronic signature;

– „**naprava za ustvarjanje kvalificiranega elektronskega podpisa**“ pomeni napravo za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II;	– "**qualified electronic signature creation device**" means an electronic signature creation device that meets the requirements laid down in Annex II;
– „**ustvarjalec žiga**“ pomeni pravno osebo, ki ustvari elektronski žig;	– "**creator of a seal**" means a legal person who creates an electronic seal;
– „**elektronski žig**“ pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov;	– "**electronic seal**" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
– „**napredni elektronski žig**“ pomeni elektronski žig, ki izpolnjuje zahteve iz člena 36;	– "**advanced electronic seal**" means an electronic seal, which meets the requirements set out in Article 36;
– „**kvalificirani elektronski žig**“ pomeni napredni elektronski žig, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega žiga in temelji na kvalificiranem potrdilu za elektronski žig;	– "**qualified electronic seal**" means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
– „**podatki za ustvarjanje elektronskega žiga**“ pomenijo enolične podatke, ki jih ustvarjalec elektronskega žiga uporabi za ustvarjanje elektronskega žiga;	– "**electronic seal creation data**" means unique data, which is used by the creator of the electronic seal to create an electronic seal;
– „**potrdilo za elektronski žig**“ pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe;	– "**certificate for electronic seal**" means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
– „**kvalificirano potrdilo za elektronski žig**“ pomeni potrdilo za elektronski žig, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge III;	– "**qualified certificate for electronic seal**" means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;
– „**naprava za ustvarjanje elektronskega žiga**“ pomeni konfigurirano programsko ali strojno opremo, ki se uporablja za ustvarjanje elektronskega žiga;	– "**electronic seal creation device**" means configured software or hardware used to create an electronic seal;
– „**naprava za ustvarjanje kvalificiranega elektronskega žiga**“ pomeni napravo za ustvarjanje elektronskega žiga, ki smiselno izpolnjuje zahteve iz Priloge II;	– "**qualified electronic seal creation device**" means an electronic seal creation device that reasonably meets the requirements laid down in Annex II;
– „**elektronski časovni žig**“ pomeni podatke v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali;	– "**electronic time stamp**" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;
– „**kvalificirani elektronski časovni žig**“ pomeni elektronski časovni žig, ki izpolnjuje zahteve iz člena 42;	– "**qualified electronic time stamp**" means an electronic time stamp which meets the requirements laid down in Article 42;
– „**elektronski dokument**“ pomeni kakršno koli vsebino, shranjeno v elektronski obliki, zlasti besedilo ali zvočni, vizualni ali avdiovizualni zapis;	– "**electronic document**" means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;
– „**storitev elektronske priporočene dostave**“ pomeni storitev, ki omogoča prenos podatkov med tretjimi stranmi z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o oddaji in prejemu podatkov, ter prenesene podatke varuje pred izgubo, krajo, poškodbo ali kakršno koli nepooblaščeno spremembo;	– "**electronic registered delivery service**" means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against loss, theft, damage or any unauthorised alterations;
– „**kvalificirana storitev elektronske priporočene dostave**“ pomeni storitev elektronske priporočene dostave, ki izpolnjuje zahteve iz člena 44;	– "**qualified electronic registered delivery service**" means an electronic registered delivery service which meets the requirements laid down in Article 44;

– „**potrdilo za avtentikacijo spletišč**“ pomeni potrdilo, ki omogoča avtentikacijo spletišča in spletišče povezuje s fizično ali pravno osebo, ki se ji izda potrdilo;

– „**kvalificirano potrdilo za avtentikacijo spletišč**“ pomeni potrdilo za avtentikacijo spletišč, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge IV;
– „**podatki za potrjevanje veljavnosti**“ pomeni podatke, ki se uporabljajo za potrjevanje veljavnosti elektronskega podpisa ali elektronskega žiga;
– „**potrjevanje veljavnosti**“ pomeni postopek preverjanja in potrditve, da je elektronski podpis ali žig veljaven.

3. KRATICE

V tem dokumentu in pripadajoči dokumentaciji, ki je v uporabi v procesu certificiranja kvalificiranih storitev zaupanja v skladu z uredbo (EU) št. 910/2014 »eIDAS«, se uporabljajo naslednje kratice:

– **CA**: Certifikacijska agencija
– **CRL**: Seznam preklicanih potrdil
– **CAB**: Organ za ugotavljanje skladnosti
– **EC**: Evropska komisija
– **EU**: Evropska unija
– **ISMS**: Sistem upravljanja informacijske varnosti
– **IT**: Informacijska tehnologija
– **TSP**: Ponudnik storitev zaupanja
– **TSL**: Lista zaupanja
– **NOD**: Nadzorni organ države sedeža TSP

– **DNS**: baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP (DNS).

– **eIDAS**: Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73).
– **ETSI**: Evropski inštitut za telekomunikacijske standarde, http://www.etsi.org, Mednarodna priporočila za področje telekomunikacij
– **HSM**: strojni varnostni modul (strojna oprema za varno shranjevanje zasebnih ključev)
– **LDAP**: Delovna skupina za spletni inženiring (protokol, ki določa dostop do imenika in je specificiran po IETF priporočilu RFC 1777 »Lightweight Directory Access Protocol«)
– **OCSP**: spletni protokol za veljavnost potrdil (protokol za sprotno preverjanje veljavnosti kvalificiranih digitalnih potrdil po priporočilu RFC 2560 »X.509 Spletni protokol za infrastrukturo javnih ključev in veljavnost potrdil)

– "**certificate for website authentication**" means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;
– "**qualified certificate for website authentication**" means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
– "**validation data**" means data that is used to validate an electronic signature or an electronic seal;

– "**validation**" means the process of verifying and confirming that an electronic signature or a seal is valid.

3. ABBREVIATIONS

In this document and the corresponding documentation which is used in the process of certifying qualified trust services in accordance with Regulation (EU) No. 910/2014 "eIDAS", the following abbreviations are used:

– **CA**: Certification Authority
– **CRL**: Certification Revocation List
– **CAB**: Conformity Assessment Body
– **EC**: European Commission
– **EU**: European Union
– **ISMS**: Information Security Management System
– **IT**: Information Technology
– **TSP**: Trust Service Provider
– **TSL**: Trust Service List
– **NOD**: Supervisory body of the country in which the TSP headquarters are located
– **DNS**: Database containing the names of computers connected to the Internet. It enables the connection of computer names with their IP numbers (DNS, Domain Name System).
– **eIDAS**: Regulation (EU) No. 910/2014 of the European Parliament and Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ES (eIDAS; Official Journal of the EU, No. L 257/73).
– **ETSI**: European Telecommunications Standards Institute, http://www.etsi.org (international recommendations for the field of telecommunications)
– **HSM**: Hardware Security Module (hardware for safe storage of private keys or hardware security module)
– **LDAP**: Internet Engineering Task Force (a protocol that enables access to the directory and is specified according to the IETF Recommendation RFC 1777 "Lightweight Directory Access Protocol"
– **OCSP**: Online Certificate Status Protocol (a protocol for prompt verification of the validity of qualified digital certificates under Recommendation RFC 2560 »X.509

– **OI**: polje v digitalnem potrdilu z imenom organizationIdentifier in OID številko 2.5.4.97, ki vsebuje identifikacijsko oznako organizacije, različno od njenega uradnega imena. Overitelj na MJU v skladu s standardi ETSI v ta namen uporablja davčno številko organizacije s predpono VATSI.

– **OID**: objektni identifikator (mednarodna številka, ki enolično določa posamezni objekt v skladu z mednarodnim standardom ITU-T X.208 (ASN.1))
– **PKCS#7** in **PKCS#10**: priporočila (kriptografski standardi za javne ključe) podjetja RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme.
– **PKCS#7** določa sintakso za kriptografsko obdelane podatke, kot so digitalni podpisi in digitalne ovojnice. Uporablja se npr. za pošiljanje digitalnih potrdil in seznamov preklicanih potrdil.
– **PKCS#10** določa sintakso zahtevka za overitev javnega ključa, imena in drugih atributov.
– **PKI**: Infrastruktura javnih ključev
– **PKIX-CMP**: določa postopek za izmenjavo podatkov, ki se nanašajo na digitalna potrdila med entitetami infrastrukture overitelja. Zajema tudi de-facto standarda PKCS#7 in PKCS#10. Objavljen je kot priporočilo RFC 4210 »Infrastruktura javnih ključev (na podlagi) X.509 – Protokoli za upravljanje s potrdili«.
– **RFC**: mednarodna priporočila za Internet skupine IETF, Delovna skupina za spletni inženiring in IESG, Vodstvena skupina za spletni inženiring, Prošnja za pripombe, http://www.ietf.org/rfc.html.
– **UTF-8**: način kodiranja mednarodnega nabora znakov unicode, pri katerem znaki ASCII ostanejo enozložni, ostali znaki pa lahko zasedajo več zlogov.

– **X.501**: priporočila za razločevalna imena: »ITU-T Priporočilo X.501 – Informacijska tehnologija – Medsebojne povezave odprtih sistemov Imenik: Modeli«.
– **X.509**: Priporočila za profil digitalnih potrdil in register preklicanih potrdil: RFC 5280: »Internet X.509 Potrdilo o infrastrukturi potrdil za javne ključe in CRL profil«.
– **TSA**: Izdajatelj varnih časovnih žigov

4. TEHNIČNI PREDPISI IN REFERENČNA DOKUMENTACIJA

V procesu certificiranja kvalificiranih storitev zaupanja v skladu z uredbo (EU) št. 910/2014 »eIDAS« Bureau Veritas uporablja naslednje tehnične predpise in referenčno dokumentacijo:

Internet Public Key Infrastructure Online Certificate Status Protocol)

– **OI**: A box in the digital certificate with the name organizationIdentifier and an OID number 2.5.4.97, which contains the identifier of the organization that differs from its official name. In accordance with ETSI standards, for this purpose the certifier at the MJU (Ministry of Public Administration) uses the tax number of the organization with VATSI as the prefix.
– **OID**: Object IDentifier (an international number which uniquely determines individual objects in accordance with the International Standard ITU-T X.208 (ASN.1))
– **PKCS#7** and **PKCS#10**: Recommendations (Public Key Cryptography Standards) of RSA Security for developers of computer systems which use asymmetric cryptographic algorithms.
– **PKCS#7**: determines the syntax for cryptographically processed data, such as digital signatures and digital envelopes. It is used e.g. for sending digital certificates and Certification Revocation Lists.
– **PKCS#10**: determines the syntax for certification requests for public keys, names and other attributes.
– **PKI**: Public Key Infrastructure
– **PKIX-CMP**: determines the procedure for exchanging data related to digital certificates among certifier infrastructure entities. It also comprises de facto standards PKCS#7 and PKCS#10. It was published as Recommendation RFC 4210 "Public Key Infrastructure (based on) X.509 Certificate Management Protocols"
– **RFC**: Request for Comments, international recommendations for internet groups entitled Internet Engineering Task Force (IETF) and Internet Engineering Steering Group (IESG), http://www.ietf.org/rfc.html.
– **UTF-8**: Method of encoding an international unicode character set, in which ASCII characters remain monosyllabic, while other characters can occupy multiple syllables.
– **X.501**: Recommendations for distinguishing names: "ITU-T Recommendation X.501 Information technology Open Systems Interconnection The Directory: Models".

– **X.509**: Recommendations for digital certificate profile and the Certificate Revocation Register: RFC 5280: »Internet X.509 Public Key Infrastructure Certificate and CRL Profile«.
– **TSA**: Time Stamping Authority (issuer of safe time stamps)

4. TECHNICAL REGULATIONS AND REFERENCE DOCUMENTATION

In the process of certifying qualified trust services in accordance with Regulation (EU) No. 910/2014 "eIDAS", Bureau Veritas uses the following technical regulations and reference documentation:

ETSI EN 319 403 V2.2.2 Elektronski podpisi in infrastrukture (ESI); Presoja skladnosti ponudnikov storitev zaupanja Zahteve organov za ugotavljanje skladnosti za presojo ponudnikov storitev zaupanja	ETSI EN 319 403 V2.2.2 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment Requirements for conformity assessment bodies assessing Trust Service Providers
SIST EN ISO/IEC 17065:2012 Zahteve za organe, ki potrjujejo izdelke, postopke in storitve	SIST EN ISO/IEC 17065:2012 Requirements for bodies certifying products, procedures and services
SIST EN ISO/IEC 17021-1:2015 Ugotavljanje skladnosti - Zahteve za organe, ki presojajo in certificirajo sisteme vodenja	SIST EN ISO/IEC 17021-1:2015 Conformity assessment Requirements for bodies providing audit and certification of management systems
UREDBA (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23. julija 2014 o elektronski identifikaciji in skrbniških storitvah pri elektronskih transakcijah na notranjem trgu in o razveljavitvi Direktive 1999/93/CE	REGULATION (EU) No. 910/2014 OF THE EUROPEAN PARLIAMENT AND COUNCIL dated 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/CE
ETSI TS 119 403-2 V1.2.1 Presoja skladnosti ponudnikov storitev zaupanja; Del 2: Dodatne zahteve organov za ugotavljanje skladnosti, ki opravljajo presojo pri ponudnikih storitev zaupanja, ki izdajajo potrdila, ki jim zaupa javnost	ETSI TS 119 403-2 V1.2.1 Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates
ETSI TS 119 403-3 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Presoja skladnosti ponudnikov storitev zaupanja; Del 3: Dodatne zahteve organov za ugotavljanje skladnosti, ki opravljajo presojo pri kvalificiranih ponudnikih storitev zaupanja v EU	ETSI TS 119 403-3 V1.1.1 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers
ETSI EN 319 401 V2.2.1 Elektronski podpisi in infrastrukture (ESI); Splošne zahteve politike za ponudnike storitev zaupanja	ETSI EN 319 401 V2.2.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1 V1.2.2 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja, ki izdajajo potrdila; Del 1: Splošne zahteve	ETSI EN 319 411-1 V1.2.2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2 V2.2.2 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja, ki izdajajo potrdila; Del 2: Zahteve za ponudnike storitev zaupanja, ki izdajajo kvalificirana potrdila za EU	ETSI EN 319 411-2 V2.2.2 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
ETSI EN 319 412-1 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Profili potrdil; Del 1: Pregled in pogoste podatkovne strukture	ETSI EN 319 412-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI EN 319 412-2 V2.1.1 Elektronski podpisi in infrastrukture (ESI); Profili potrdil; Del 2: Profil potrdil, izdanih fizičnim osebam	ETSI EN 319 412-2 V2.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI EN 319 412-3 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Profili potrdil; Del 3: Profil potrdil, izdanih pravnim osebam	ETSI EN 319 412-3 V1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
ETSI EN 319 412-4 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Profili potrdil; Del 4: Profil potrdil, izdanih spletiščem	ETSI EN 319 412-4 V1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
ETSI EN 319 412-5 V2.2.1 Elektronski podpisi in infrastrukture (ESI); Profili potrdil; Del 5: Izjave o KK	ETSI EN 319 412-5 V2.2.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements

ETSI EN 319 421 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja, ki izdajajo časovne žige	ETSI EN 319 421 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI EN 319 422 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Protokol časovnih žigov in profilov kuponov za časovne žige	ETSI EN 319 422 V1.1.1 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
ETSI EN 319 521 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev elektronske priporočene dostave	ETSI EN 319 521 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
ETSI EN 319 522-1 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 1: Okvir in arhitektura	ETSI EN 319 522-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture
ETSI EN 319 522-2 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 2: Semantična vsebina	ETSI EN 319 522-2 V1.1.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents
ETSI EN 319 522-3 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 3: Formati	ETSI EN 319 522-3 V1.1.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats
ETSI EN 319 522-4-1 V1.2.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 4: Vezave; Poddel 1: Vezave pri dostavi sporočil	ETSI EN 319 522-4-1 V1.2.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Del 4: Bindings; Sub-part 1: Message delivery bindings
ETSI EN 319 522-4-2 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 4: Vezave; Poddel 2: Vezave dokazov in identifikacij	ETSI EN 319 522-4-2 V1.1.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings
ETSI EN 319 522-4-3 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene dostave; Del 4: Vezave; Poddel 3: Vezave sposobnosti ali zahtev	ETSI EN 319 522-4-3 V1.1.1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings
ETSI EN 319 531 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev elektronske priporočene pošte	ETSI EN 319 531 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers
ETSI EN 319 532-1 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene pošte (REM); Del 1: Okvir in arhitektura	ETSI EN 319 532-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture
ETSI EN 319 532-2 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene pošte (REM); Del 2: Semantična vsebina	ETSI EN 319 532-2 V1.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents
ETSI EN 319 532-3 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene pošte (REM); Del 3: Formati	ETSI EN 319 532-3 V1.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats
ETSI EN 319 532-4 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Storitve elektronske priporočene pošte (REM); Del 4: Profili interoperabilnosti	ETSI EN 319 532-4 V1.1.1 Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles
ETSI TR 119 000 v1.2.1 Elektronski podpisi in infrastrukture (ESI); Okvir za standardizacijo podpisov: pregled	ETSI TR 119 000 v1.2.1 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview
ETSI TR 119 001 V1.2.1 Elektronski podpisi in infrastrukture (ESI); Okvir za standardizacijo podpisov: pregled; Definicije in kratice	ETSI TR 119 001 V1.2.1 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations

ETSI TR 119 400 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Smernica o uporabi standardov za ponudnike storitev zaupanja s podporo digitalnim podpisom in sorodnim storitvam
ETSI TR 119 411-4 v1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja, ki izdajajo potrdila; Del 4: Kontrolni seznam za podporo presoji TSP glede ETSI EN 319 411-1 ali ETSI EN 319 411-2
ETSI TS 119 101 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za aplikacije za ustvarjanje in potrjevanje veljavnosti podpisov
ETSI TS 119 431-1 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja; Del 1: Deli za storitve TSP, ki upravljajo QSCD/SCDev na daljavo
ETSI TS 119 431-2 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike in varnostne zahteve za ponudnike storitev zaupanja; Del 2: Deli za storitve TSP, ki podpirajo ustvarjanje digitalnih podpisov AdES
ETSI TS 119 441 V1.1.1 Elektronski podpisi in infrastrukture (ESI); Zahteve politike za TSP, ki nudijo storitve potrjevanja veljavnosti podpisov
ETSI TS 119 495 V1.3.1 Elektronski podpisi in infrastrukture (ESI); Za sektor specifične zahteve; Profili kvalificiranih potrdil in zahteve politike TSP v skladu z Direktivo (EU) 2015/2366 o plačilnih storitvah
ISO/IEC 27001:2013 "Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti -Zahteve".
ISO/IEC 27002:2013 " Informacijska tehnologija – Varnostne tehnike – Kodeks prakse za kontrole informacijske varnosti".
ISO/IEC 27006:2015 "Informacijska tehnologija – Varnostne tehnike – Zahteve za organe, ki nudijo presojo in certificiranje sistemov upravljanja informacijske varnosti"
ISO/IEC TS 27008:2019 Informacijska tehnologija – Varnostne tehnike – Smernice za presojo kontrol informacijske varnosti

ETSI TR 119 400 V1.1.1 Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for trust service providers supporting digital signatures and related services
ETSI TR 119 411-4 v1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2
ETSI TS 119 101 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
ETSI TS 119 431-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
ETSI TS 119 431-2 V1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation
ETSI TS 119 441 V1.1.1 Electronic Signatures and Infrastructures (ESI);Policy requirements for TSP providing signature validation services
ETSI TS 119 495 V1.3.1 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
ISO/IEC 27001:2013 "Information technology -Security techniques -Information security management systems - Requirements".
ISO/IEC 27002:2013 "Information technology -Security techniques -Code of practice for information security controls".
ISO/IEC 27006:2015 "Information technology -Security techniques -Requirements for bodies providing audit and certification of information security management systems"
ISO/IEC TS 27008:2019 Information technology Security techniques Guidelines for the assessment of information security controls

5. SPLOŠNI POGOJI

(Obveznosti Bureau Veritas d.o.o.) BV omogoča neomejen dostop do svojih storitev vsem organizacijam, ki zaprosijo za certifikacijo po Uredbi (EU) št. 910/2104 brez kakršnega koli razlikovanja. Bureau Veritas si pridržuje pravico do zavrnitve vloge ali do prekinitve pogodbe o certificiranju s stranko na podlagi utemeljenih razlogov, o čemer mora stranko tudi obvestiti. Dostop do certificiranja ni odvisen od velikosti organizacije ali od njene pripadnosti nekemu združenju ali skupini, prav tako pa za certificiranje ni pogoj število že opravljenih certifikacij.

5. GENERAL TERMS AND CONDITIONS

(Obligations of Bureau Veritas d.o.o.) BV enables unlimited access to its services for all organizations requesting certification under Regulation (EU) No. 910/2104, without any discrimination. However, Bureau Veritas reserves the right to reject an application or to terminate a certification agreement with a Client for well-founded reasons, and shall be obliged to inform the Client thereof. Access to certification does not depend on the size of the organization or its affiliation with any association or group. Certification is also not conditional upon the number of already completed certifications.

Cenik certifikacije se oblikuje glede na sredstva, ki so dejansko potrebna za izvajanje storitve. Cenik in njegovo uporabo nadzoruje vodja certifikacijskega organa.

BV se zavezuje, da ne bo izvajal svetovalnih dejavnosti in da bo zagotavljal, da presojevalci niso v pogodbenem razmerju z zainteresiranimi organizacijami oz. družbami v obdobju dveh let pred izvedbo storitve in v obdobju dveh let po tem.
Odločitve BV o certificiranju temeljijo na skupni oceni celotnega procesa presoje, v katerega so zajeti objektivni dokazi, preizkusi in preverjanja, izvedena v obliki začetne in certifikacijske presoje pred priporočilom za odobritev certificiranja in po njej. BV ne garantira uspešnega izida odločitve o odobritvi certificiranja oziroma izdaje ustreznega certifikata po opravljeni presoji. Ker se objektivni dokazi o skladnosti pridobivajo na podlagi vzorčenja, njihov pozitiven rezultat sam po sebi še ne zagotavlja skladnosti z vsemi predpisanimi zahtevami.

BV se zaveda pomena nepristranskosti pri certificiranju, zato je pri opravljanju svojih nalog objektiven in se izogiba morebitnim navzkrižjem interesov. Nadzor nad ohranjanjem nepristranskosti pri BV opravlja poseben Certifikacijski odbor, ki zastopa stranke, zainteresirane za certificiranje.

(**Obveznosti organizacije**) Stranka, ki se prijavi v postopek certificiranja, se zavezuje:
(a) da bo pri izvajanju vseh svojih storitev izpolnjevala zahteve za certificiranje;
(b) da bo omogočala začetno certificiranje in izvedbo kontrolnih presoj ter presoj na podlagi posredovanih sprememb, da bo BV predložila vso zahtevano dokumentacijo ter omogočila dostop do vseh dokumentiranih informacij ter da bo BV omogočala dostop do lokacij, naprav in, če bi bilo potrebno, svojih podizvajalcev za potrebe izvede presoj skladno z zakonsko veljavnimi pogoji in ob spoštovanju lastnih postopkov;

(c) da bo pri presojanju omogočala udeležbo opazovalcev (presojevalci pripravniki BV, predstavniki NOD in predstavniki akreditacijskih organov) skladno z zakonsko veljavnimi pogoji in ob spoštovanju lastnih postopkov;

(d) da bo omogočila presojevalcem pripravnikom, tehničnemu osebju BV in njihovim predstavnikom, kot tudi predstavnikom akreditacijskih ustanov in/ali predstavnikom NOD, dostop do kateregakoli dela presoje ali procesa presoj z namenom, da se preverja skladnost dela presojevalcev BV z ustreznimi standardi akreditacijskih organov.

The price list for certifications is formed on the basis of the means actually required to perform this service. The price list and the application thereof are supervised by the certification body's director.
BV undertakes not to perform consulting activities and to make sure that the auditors are not contractually related to interested organizations or companies for a period of two years before and two years after this service is provided.

Decisions of BV related to certification are based on the overall assessment of the total audit process, which includes objective evidence, testing and verifications performed in the form of initial and certification audit before and after recommendations to approve certification. BV does not guarantee a successful outcome of the decision to approve certification or the issuance of an appropriate certificate when the audit has been completed. Since objective evidence on conformity is obtained on the basis of sampling, its positive result in and of itself does not guarantee conformity with all of the prescribed requirements.
BV is well aware of the significance of an impartial approach to the certification process. Therefore, in the performance of its tasks, BV is objective and avoids any conflict of interest. At BV, the maintenance of impartiality is overseen by a special Certification Committee, which represents clients interested in being certified.

(**Obligations of the organization**) The client applying for the certification procedure hereby undertakes:
(a) to meet the certification requirements in the provision of all of its services;
(b) to enable initial certification and the performance of surveillance audits and audits on the basis of the communicated changes, to submit all of the required documentation to BV, and to give it access to all of its documented information, as well as to give BV access to its locations, equipment and, if necessary, also its subcontractors for the needs of performing its audits in accordance with the legally applicable conditions and in line with its own procedures;
(c) to enable the participation of observers in the performance of audits (trainee auditors at BV, as well as NOD representatives and representatives of accreditation bodies) in accordance with the legally applicable conditions and in line with its own procedures;
(d) to enable trainee auditors, the technical staff of BV, and its representatives, as well as the representatives of accreditation bodies and/or NOD representatives, access to any part of the audit or the audit process in order to check whether the work done by BV auditors is in line with the relevant standards of accreditation bodies.

(e) da bo evidentirala reklamacije, omogočala BV vpogled v tovrstne evidence in da bo reklamacije reševala z ustreznimi korektivnimi ukrepi;
(f) da bo BV obveščala o vseh spremembah pri izvajanju storitev zaupanja, ki bo na osnovi presoje odločila ali so za ohranitev certificiranja potrebne dodatne presoje. Obveščanje mora potekati na elektronski naslov eidas-slovenia@bureauveritas.com ;
(g) da za izvajanje bistvenih storitev (npr.: upravljanje s strojnimi varnostnimi moduli HSM; upravljanje s preklicanimi seznami za potrdila CRL; upravljanje s prijavno službo overitelja), ne bo uporabljala storitev zunanjih nekvalificiranih ponudnikov storitev zaupanja (ki ne bi ustrezali definiciji QTSP (Qualified Trusted Service Provider);
(h) da bo pri kvalificiranih ponudnikih storitev zaupanja QTSP, ki bi vključevali enega ali več strojnih varnostnih modulov – HSM namenjene izvajanju kvalificiranih storitev organizacije, organizacija morala zagotoviti ustrezne kriterije za monitoring in operativni nadzor teh naprav, si pri njih zagotoviti pravico do izvedbe presoje ter poskrbeti, da bodo presojevalci certifikacijskega organa, predstavniki NOD in ocenjevalci Slovenske Akreditacije imeli odobren dostop do teh naprav. Poleg navedenega mora organizacija zahtevati, da bo pri kvalificiranih ponudnikih storitev zaupanja QTSP, ki bi vključevali enega ali več strojnih varnostnih modulov – HSM namenjene izvajanju kvalificiranih storitev zaupanja organizacije, informacijska varnost temeljila na sistemu upravljanja informacijske varnosti in je tak QTSP nosilec veljavnega akreditiranega ISO/IEC 27001 certifikata;

(i) da bo ohranjala ustrezno višino finančnih sredstev in/ali sklenila ustrezno zavarovalno polico za civilno odgovornost, pri kateri bo upoštevan najvišji združljiv znesek izgub za posamezen dogodek, ki bi bil povezan s potencialnim napačnim ravnanjem in številom strank z navedeno vrednostjo transakcij;
(j) da bo hranila poročilo o presoji najmanj 4 leta in ga bo v 3 (treh) dneh po prejemu posredovala NOD za nadaljevanje postopkov odločitve o določitvi organizacije kot kvalificiranega ponudnika storitev zaupanja (QTSP) in o vpisu organizacije na »Listo zaupanja« (Trusted List).

(Obvezujoči predpisi in certifikacijske omejitve) BV se zavezuje, da bo z vzorčenjem preverjal, ali organizacija zagotavlja skladnost storitev zaupanja, ki se certificirajo, organizacija pa je sama odgovorna za pravilno izvajanje svojih aktivnosti, za upoštevanje zakonskih obveznosti, povezanih s storitvami zaupanja, ki jih izvaja, in pogodbenih obveznosti do svojih strank.

(e) to record any complaints and enable BV to view any such records, as well as to resolve complaints with appropriate corrective actions;
(f) to inform BV of any changes in the performance of trust services, whereby BV shall determine on the basis of its assessment whether any additional audit is needed to maintain certification. Such notices shall be sent to the e-mail address eidas-slovenia@bureauveritas.com;
(g) not to use the services of external non-qualified trust service providers (which would not fit the definition of a QTSP (Qualified Trusted Service Provider) for the implementation of the essential services (e.g. management of Hardware Security Modules (HSM); management of Certification Revocation Lists (CRL); management of the certifier's application service);
(h) that for qualified trust service providers (QTSP) which would include one or more Hardware Security Modules (HSM) intended for the performance of the organization's qualified services, the organization shall provide the appropriate criteria for the monitoring and operative supervision of this equipment, make sure that it has the right to perform audits at such service providers, and make sure that the certification body's auditors, NOD representatives and representatives of the Slovenian Accreditation have been approved access to this equipment. In addition to the above, the organization shall demand that for qualified trust service providers (QTSP) which would include one or more Hardware Security Modules (HSM) intended for the performance of the organization's qualified services, information security would be based on an information security management system and such QTSP would be the holder of a valid accredited ISO/IEC 27001 certificate;
(i) to maintain an appropriate amount of monetary funds and/or conclude an appropriate insurance policy for civil liability, taking into account the highest aggregate amount of loss for each individual event relating to potential misconduct and the number of clients with the stated value of transactions;
(j) to keep each audit report for at least 4 years and submit it to NOD within 3 (three) days of receipt thereof for continued procedures to verify whether an organization should be identified as a qualified trust service provider (QTSP) and include it on the Trusted List.

(Compulsory regulations and certification limitations) BV undertakes to check by sampling whether the organization ensures conformity of its trust services undergoing certification, and the organization itself shall be responsible for correct performance of its activities, for its conformity with the legal obligations relating to the trust services it provides, and with its contractual obligations to its own customers.

(Registracija in zaupnost podatkov) BV bo s podatki, pridobljenimi v postopkih certificiranja, ravnala zaupno. Te podatke lahko razkrije le v zakonsko določenih primerih in, kadar gre za akreditirane sheme, akreditacijskim organom in pristojnemu NOD. Podatki, povezani z organizacije, se hranijo najmanj 4 (štiri) leta in v celotnem ciklu trenutne certifikacije ter za predhodni certifikacijski cikel v primeru ponovne certifikacije ali dlje če so take zakonske zahteve.

(Registration and confidentiality) BV shall maintain the confidentiality of any data it obtains during its certification processes. Such data may be disclosed only in legally stipulated cases and, when accredited schemes are involved, also to the accreditation bodies and the competent NOD. Data associated with the organization shall be kept for at least 4 (four) years and over the entire cycle of the current certification, as well as for the previous certification cycle in the case of re-certification, or even longer if this is required by law.

(Trajanje pogodbe) Pogodba začne veljati z dnem, ko jo podpišeta obe pogodbeni stranki, in je veljavna do izteka določenega v pogodbi. Pri pogodbi se poleg pogojev, navedenih v teh splošnih pravilih, smiselno upoštevajo tudi splošni pogoji opravljanja storitev BV.

Pogodba se razveljavi, če v enem letu od njene sklenitve zahtevanega certifikata ne bi bilo mogoče izdati, razlogov za to pa ne bi bilo mogoče pripisati BV, in ob preklicu ali umiku certifikata.

(Term of the agreement) The agreement shall come into force on the day when it is signed by both parties and shall remain in force until the expiry of the time period determined in the agreement. In addition to the terms and conditions stated in these General Rules, the general terms and conditions for BV services shall also be reasonably taken into account in the agreement.
The agreement shall be annulled if the required certificate cannot be issued within one year of its conclusion and the reasons for this are not attributable to BV, as well as upon any certificate revocation or withdrawal.

6. FORMALNI POSTOPEK CERTIFICIRANJA

Zainteresirana organizacija zaprosi BV za pripravo ponudbe, pri čemer ji bistvene podatke posreduje v posebnem vprašalniku. Ti podatki morajo zajemati:

a) storitve družbe/izdelke, za katere se zahteva certificiranje;
b) certificiranje(-a), ki je/so predmet zahtevka(-ov) eIDAS
c) in druge elemente, navedene v vprašalniku.

BV pregleda popolnost prejetih informacij, pri sebi preveri zmožnost izvedbe navedene storitve v zahtevanih terminih in zainteresirani organizaciji pošlje ponudbo, v kateri bo, če bo ponudba sprejeta, opredeljen tudi njen ekonomski vidik.
Ponudba zajema vse stroške procesa certificiranja, vključno s stroški certifikacijske presoje in stroški kontrolnih presoj, usmerjenih v ohranjanje veljavnosti certifikata v celotnem obdobju certifikacijskega cikla (dve leti) in njegovi obnovi.
Pri določitvi časovnih okvirov, potrebnih za izvedbo presoje, BV uporablja smernice akreditacijskega organa, ki med drugim upoštevajo tudi:

- obseg certificiranja ponudnika storitev zaupanja (TSP, na primer: št. uporabljenih informacijskih sistemov, št. zaposlenih, št. izdanih certifikatov);
- kompleksnost organizacije;
- vrste poslov v okviru predvidenega namena;

6. FORMAL CERTIFICATION PROCEDURE

An interested organization may ask BV to prepare an offer, and it shall provide the essential data via a special questionnaire. These data shall include:

a) the company's products/services for which certification is requested;
b) the certification(s), which is (are) the subject of eIDAS request(s)
c) and any other elements stated in the questionnaire.

BV shall review the completeness of received information, check its own ability to provide the required service within the requested time frame and send an offer to the interested organization, in which, should such offer be accepted, its economic aspects shall also be defined.
The offer shall include all of the costs of the certification process, including the costs of certification audits and the costs of surveillance audits aimed at maintaining the certificate's validity over the entire duration of the certification cycle (two years) and its renewal. In determining the timeframes required to perform the audit, BV shall apply the accreditation body's guidelines which among other things also take into account the:

- scope of certification of the trust service provider (TSP, for example, the number of used information systems, the number of employees and the number of issued certificates);
- complexity of the organization;
- types of business transactions within the planned purpose;

- obseg in vrste tehnologije, ki se uporabljajo pri izvajanju različnih komponent storitev zaupanja;
- število lokacij;
- obseg zunanjih ponudnikov (outsourcinga) in tretjih oseb v okviru namena posamezne storitve zaupanja;
- obstoječe certifikate.

(Začetna / Certifikacijska presoja) Dejavnosti, predvidene za dvoletni certifikacijski cikel, vključujejo prvo certificiranje, ki se opravi v dveh fazah (Stage 1 in Stage 2) in zajema začetno presojo (Stage 1) in certifikacijsko presojo (Stage 2) ter kontrolno presojo (ki mora biti izvedena v okviru +/-30 dni od izračunanega datuma kontrolne presoje (zadnji dan (re)-certifikacijske presoje + 365 (tristopetinšestdeset dni)), ki se opravi enkrat letno, in re-certifikacijo presojo, ki mora biti izvedena pravočasno (vsaj 90 dni pred iztekom veljavnosti certifikata).
Za izvedbo presoj BV imenuje presojevalsko ekipo, o kateri pravočasno obvesti stranko. BV izvede določitev presojevalske ekipe z upoštevanjem ustrezne strokovne usposobljenost posameznih članov presojevalske ekipe in odsotnost njihovih dejanskih ali potencialnih navzkrižij interesov ali vlog. Organizacija lahko, če ima za to utemeljen razlog, zaprosi za delno ali celotno zamenjavo članov presojevalske ekipe, pri čemer mora svoje razloge navesti v pisni obliki. Presojevalsko ekipo lahko sestavljajo tudi člani/presojevalci in/ali tehnični eksperti, ki niso zaposleni pri BV, pri čemer je za njihovo delovanje odgovoren BV. Tehnični ekspert (i) zagotavlja presojevalski ekipi posebna znanja ali strokovno pomoč v postopku presoje, ter se ne šteje kot presojevalec. Tehnični ekspert (i) so vedno odgovorni vodji presojevalske ekipe.

(Predmet presoje) Cilj presoje je preveriti, ali so zahteve navedene v Uredbi (EU) št. 910/2014 in relevantnih ETSI EN standardih izpolnjene.
Presoja se izvede izključno za storitve zaupanja navedene v uvodni fazi predložitve vloge. Po potrebi se lahko prvotni obseg spremeni, do začetka Stage 2 presoje, vendar je potreben ponoven izračun potrebnega časa za izvedbo presoje in morebitno spremembo pogodbe. Presoja se izvede na lokaciji (ah) izvajanja storitev zaupanja v obliki neposrednega ali/in oddaljenega nadzora, s katerim se bo ugotavljala skladnost izvajanja storitev zaupanja z zahtevami navedene v Uredbi (EU) št. 910/2014 in relevantnih ETSI EN standardih.

(Kontrolne presoje) V obdobju veljavnosti certifikata BV izvaja kontrolne presoje, katerih cilj je ovrednotiti ohranjanje pogojev delovanja glede na pogoje, ki so omogočili prvotno izdajo certifikata. Ta dejavnost se izvaja

- scope and types of technologies used in the implementation of various trust service components;
- number of sites;
- scope of external contractors (outsourcing) and third parties within the purpose of each individual trust service;
- the existing certificates.

(Initial/Certification audit) The activities envisaged for the two-year certification cycle include the first certification, which is done in two stages (Stage 1 and Stage 2) and comprises the initial audit (Stage 1), the certification audit (Stage 2) and surveillance audit (which shall be done within +/-30 days of the calculated date of surveillance audit (last day of the (re)-certification audit + 365 (three hundred and sixty-five days)), which is done once a year, and a re-certification audit which shall be done on a timely basis (at least 90 days before certificate expiry).
For the performance of these audits, BV shall appoint an audit team, and shall inform the client of this on a timely basis. BV shall compose this audit team taking into account the corresponding professional qualifications of the individual audit team members and the absence of their actual or potential conflicts of interests or roles. If it has a well-founded reason to do so, the organization may request a partial or total replacement of audit team members, whereby its reasons for this should be stated in writing. The audit team may also be composed of members/auditors and/or technical experts who are not employed at BV, whereby BV shall be responsible for their work. The technical expert (s) shall provide the audit team with special knowledge or professional assistance in the audit process and shall not be deemed one of the auditors. The technical expert(s) shall always report to the audit team leader.

(Subject of audit) The objective of audit shall be to check whether the requirements from Regulation (EU) No. 910/2014 and the relevant ETSI EN standards have been met.
Audit shall be done exclusively for the trust services stated in the initial stage of filing the application. If necessary, the initial scope may be changed by the beginning of Stage 2 of the audit, but the time needed to complete the audit has to be re-calculated and the agreement shall be changed as necessary. The audit shall be conducted at a location(s) at which the trust services are provided in the form of on site or/and remote audit, with which conformity of the provision of trust services with the requirements of Regulation (EU) No. 910/2014 and the relevant ETSI EN standards will be audited.

(Surveillance audits) During the period of a certificate's validity, BV shall perform periodic surveillance audits, the purpose of which is to evaluate continued conformity with the operating conditions, compared to the ones which enabled

na sedežu organizacije in izbranih lokacijah, če te obstajajo. Pogostost opravljanja teh presoj, ki je odvisna od programa presoj, za prvi certifikacijski cikel pa je določen v vsakokrat veljavni pogodbi.

Kontrolne presoje se izvajajo in ugotovitve se dokumentirajo v poročilu.

(Rezultati presoj) Ob koncu vsake posamezne presoje bo vodja presoje poročal na zaključnem sestanku o ugotovitvah presoje ter morebitna poročila o ugotovljenih neskladnostih predal organizaciji, celotno poročilo presoje pa bo dostavil v roku 5 (pet) delovnih dni od zaključnega sestanka.

(Neskladnosti)
Odobritev certificiranja z odprtimi neskladnostmi pri ni dovoljena. Implementacija ustreznih korektivnih ukrepov mora biti preverjena pred odobritvijo certificiranja.

Vodja presoje določi skrajni rok za odpravo vseh neskladnosti tako, da so korektivni ukrepi v celoti uvedeni pred priporočilom za prvo odobritev certificiranja ali iztekom veljavnosti obstoječega certifikata.

Korektivni ukrepi za odpravo neskladnosti se morajo pričeti izvajati takoj. Korekcija, analiza vzrokov in korektivni ukrepi, skupaj z ustreznimi dokazili o uvedbi/izvajanju, morajo biti predloženi najkasneje v roku 80 dni od zadnjega dne presoje. Za odpravo ugotovljenih neskladnosti je na razpolago največ 90 dni od zadnjega dne presoje. Postopki pregleda ustreznosti predloženih korektivnih ukrepov in interni postopki odobritve certificiranja trajajo najmanj 10 dni. V primerih, ko je obdobje med datumom presoje in datumom veljavnosti certifikata krajše od 90 dni, se 90 dnevni rok za odpravo vseh neskladnosti ustrezno skrajša, če želi ponudnik storitev zaupanja obdržati kontinuiteto certificiranja.

Vse odgovore in dokumente o izvedenih korektivnih ukrepih na ugotovljene neskladnosti ponudnik storitev zaupanja pošlje v pisarno BV Dokumenti so lahko v elektronski (zaželeno) ali papirnati obliki. Dokazila, da je bil korektivni ukrep za odpravo neskladnosti izveden in je uspešen morajo biti predložena presojevalcu v pregled.

Pregled dokumentacije o vseh neskladnostih presojevalec opravi v pisarni (desktop review). V odvisnosti od resnosti ugotovljenih neskladnosti se presojevalec lahko odloči za

the initial issuance of the certificate. This activity shall be performed at the headquarters of the organization and at selected locations, if any exist. The frequency of such surveillance audits, which depends on the surveillance audits program for the first certification cycle, shall be determined in the initial and after valid agreement.
Each surveillance audit shall be performed and its findings shall be documented in a report.

(Results of audits) At the end of each individual audit, the audit team leader shall report on the findings of the audit at the final meeting and shall provide any reports on established non-conformities to the organization. The complete audit report shall be delivered to the client within 5 (five) business days of the final meeting.

(Non-conformity)
Approval of certification with an unresolved non-conformity shall not be permitted. The implementation of appropriate corrective actions shall be verified before certification may be approved.
The audit team leader shall determine the ultimate time limit for resolving all non-conformities, so that the corrective actions shall be implemented in their entirety before a recommendation is made for first approval of certification or before the expiry of an existing certificate.
The corrective actions to eliminate non-conformities shall begin to be implemented immediately. The correction, analysis of the causes, and corrective actions, along with appropriate evidence on their implementation/performance shall be submitted at the latest within 80 days of the last day of the audit. To eliminate any established non-conformity, a maximum of 90 days from the last day of the audit shall be granted. The procedures for assessing the appropriateness of the proposed corrective actions and internal procedures for certification approval shall last at least 10 days. In cases in which the period between the date of the audit and date of certificate expiry is shorter than 90 days, the said 90-day time limit for the elimination of any and all non-conformities shall be appropriately shorter if the trust service provider wishes to maintain the continuity of the certification.
All of the replies and documents on the implemented corrective actions regarding an established non-conformity shall be sent by the trust service provider to the office of BV These documents may be provided either in electronic form (preferably) or as hard copy. The evidence proving that a particular corrective action for the elimination of a non-conformity was performed and was effective shall be submitted to the auditor for review.
A review of the documentation on all non-conformities shall be done by an auditor in his/her office (desktop review). Depending on the severity of the established non-conformity,

dodatno presojo (follow up), na kateri preveri uvedene korektivne ukrepe, oceni njihovo uspešnost in odloči ali se lahko predlaga odobritev certificiranja oziroma nadaljevanje certificirana ali pa zahteva dodatne dopolnitve, ki morajo biti ponovno predložene v pregled.

Odziv ponudnika storitev zaupanja na ugotovljene neskladnosti pregleda presojevalec v štirih delih: korekcija, analiza vzrokov, korektivni ukrepi in preverjanje učinkovitosti uvedenih korektivnih ukrepov. Pri pregledu teh delov, presojevalec išče ukrepe za odpravo neskladnosti in ali se v praksi izvajajo.

Korekcija

1. Obseg neskladnosti je določen (neskladnost je bila odpravljena, ponudnik storitev zaupanja je raziskal sistem(e) in preveril ali obstajajo še drugi primeri, ki jih mora popraviti oz. odpraviti). Prepričati se je potrebno ali korekcija odgovarja na vprašanje: "Ali je to osamljen primer ali ne?". Z drugimi besedami: "Ali obstaja možnost, da se podobno pojavi še kje drugje, v drugi storitvi zaupanja, drugem procesu, na drugi lokaciji, drugem oddelku, pri drugem ponudniku storitev zaupanja, ki se uporabljajo za izvajanje storitev zaupanja?

2. Če korekcija ne more biti izvedena takoj, je potrebno pripraviti plan za odpravo neskladnosti, ki vsebuje rok, ki ni daljši od 90 dni od izdaje neskladnosti in odgovorno osebo.

3. Dokazila, da je bila korekcija izvedena in je uspešna morajo biti predložena presojevalcu v pregled.

Analiza vzrokov

1. Temeljni vzrok ni samo ponovitev ugotovitve (neskladnosti), niti ni neposredni vzrok težav.

2. Temeljni vzrok je mogoče ugotoviti samo s poglobljeno analizo: npr. nekdo ni upošteval navodil pri procesu to je neposredni vzrok; ugotavljanje zakaj nekdo ni upošteval navodil, pa nas lahko pripelje do temeljnega vzroka.

3. Opis temeljnega vzroka mora biti osredotočen in jasen ter ne sme dopuščati dodatnih vprašanj "zakaj". Če si pri analizi vzrokov lahko upravičeno zastavimo vprašanje "zakaj", le to pomeni, da analiza ni bila dovolj poglobljena.

4. Prepričajte se, da analiza vzroka odgovarja na vprašanje, "Kaj v sistemu je bilo narobe, da je prišlo do problema oz. nepravilnosti?"

Korektivni ukrep

1. Korektivni ukrep mora obravnavati temeljne vzroke ugotovljene ob analizi vzrokov. Če niste določili resničnega temeljnega vzroka, ne morete preprečiti ponovitve problema.

the auditor may decide to perform an additional audit (follow up), at which the implemented corrective action shall be checked, its efficacy shall be assessed and a decision shall be made on whether to propose certification approval or continued certification, or whether additional supplements shall be required which shall be re-submitted for review.

The trust service provider's response to an established non-conformity shall be reviewed by an auditor in four parts: correction, analysis of causes, corrective actions, and verification of the effectiveness of implemented corrective actions. When reviewing these parts, the auditor searches to find measures to eliminate the non-conformity and investigates whether these have been implemented in practice.

Correction

1. The scope of non-conformity shall be determined (the non-conformity was eliminated, the trust service provider has examined the system(s) and checked if there were any other cases that needed to be remedied or eliminated). It is necessary to verify whether the correction is a reply to the question: "Is this an isolated case or not?". In other words: "Is there a possibility that something similar may happen anywhere else, in another trust service, in another process, at another location, in another department, or with another trust service provider, used to perform trust services?

2. If a correction cannot be done immediately, a plan for eliminating the non-conformity has to be prepared, comprising a time limit not longer than 90 days of the issuance of such non-conformity and a responsible person.

3. Evidence that a correction was performed and was effective *shall be submitted to the auditor for review.*

Analysis of causes

1. The basic cause is not just a repetition of the finding (of non-conformity), and neither is it a direct cause of the problems.

2. The basic cause can be established only with an in-depth analysis: e.g. someone did not observe the instructions for the process – this would be a direct cause; and finding out why someone did not observe the instructions may then lead us to the base cause.

3. Description of the basic cause shall be focused and clear and shall not allow for any further questions of "Why". If in the analysis of causes one can justifiably pose the question of "Why", this means that the analysis of causes was not deep enough.

4. Verify that the analysis of causes answers the question of "What in the system went wrong, so that this problem or irregularity occurred?"

Corrective action

1. A corrective action shall address the base causes established during the analysis of causes. If the actual base cause was not established, the problem cannot be prevented from recurring.

2. Če korektivni ukrep ne more biti izveden takoj, je potrebno pripraviti plan za odpravo neskladnosti, ki vsebuje rok, ki ni daljši od 90 dni od izdaje neskladnosti in odgovorno osebo.
3. Vedno vključuje spremembe storitve zaupanja, sistema, dodatno usposabljanje, spremembe postopkov, dodatne kontrole in druge ukrepe, ki preprečujejo ponovitev neskladnosti.
4. Dokazila, da je bil korektivni ukrep za odpravo neskladnosti izveden in je uspešen morajo biti predložena presojevalcu v pregled.
Preverjanje uspešnosti uvedenih ukrepov
1. Preverjanje uspešnosti uvedenih ukrepov mora biti izvedeno po uvedenih ukrepih. V primerih, ko se ugotovi, da ukrepi ne dajejo rezultatov, jih je potrebno na re-definirati in ponovno izvesti celoten postopek od analize vzrokov do ponovnega preverjanja uspešnosti uvedenih ukrepov.

2. If a corrective action cannot be performed immediately, it is necessary to prepare a plan to eliminate any non-conformity, comprising a time limit not longer than 90 days of the issuance of non-conformity, and a responsible person.
3. Always include any changes in the trust service, system, additional training, changes in procedures, additional surveillance and other measures which prevent such non-conformity from recurring.
4. Evidence proving that the corrective action for the elimination of a non-conformity was implemented and was also effective shall be submitted to the auditor for review.
Verification of the efficacy of implemented measures
1. Once the measures have been implemented, the verification of their efficacy shall be done. In the cases where it is found that the said measures did not produce results, they need to be redefined and the entire procedure shall be done again, from the analysis of causes to repeated verification of the efficacy of implemented measures.

(Odobritev certificiranja) Za odločitev v zvezi z odobritvijo certificiranja je pristojen vodja certifikacijskega organa BV, ki bo za to ponovno pregledal celoten postopek in vse pridobljene informacije. Odobritev certificiranja pri še neodpravljenih neskladjih ne bo izvedena.

Vodja certifikacijskega organa lahko:
(a) odobri certificiranje in dovoli izdajo certifikata za kvalificirane storitve zaupanja, ki so skladne z zahtevami;

(b) začasno odobri izdajo certifikata, če so bile izdane neskladnosti, ki ne vplivajo na izvajanje storitve zaupanja, vendar največ za 90 dni za kvalificirane storitve zaupanja, ki so skladne z zahtevami.

(c) Ne odobri izdaje certificiranja.
Vodja certifikacijskega organa izda svoj sklep na osnovi dokazil, s katerimi je bil do tistega trenutka seznanjen, lahko pa kadar koli odloči, da bi bilo treba izvesti dodatna preverjanja, če bi bilo po njegovi presoji to potrebno.
Certificiranje, ki ga odobri BV kvalificiranemu ponudniku storitev zaupanja (QTSP), ne zagotavlja, da bo NOD uvrstil ponudnika storitev zaupanja (QTSP) na listo zaupanja (TSL).

(Approval of certification) The director of the certification body with BV shall be competent to pass the decision on the approval of certification. For this purpose, the said director shall do a repeat review of the entire procedure and all of the acquired information. In the case where non-conformity has not yet been eliminated, the approval of certification may not be issued.
The certification body's director may:
(a) approve the certification and permit the issuance of the certificate for those qualified trust services which are compliant with the requirements;
(b) temporarily approve the issuance of the certificate if a non-conformity was established that does not affect the performance of the trust services; this may be done within 90 days at a maximum for qualified trust services which are compliant with the requirements.
(c) not approve the issuance of the certificate.
The certification body's director shall issue his/her own decision based on the evidence received by that moment, but he/she may decide at any time that additional checking is needed if necessary in his/her opinion.
The certification approved by BV for a qualified trust service provider (QTSP) does not guarantee that the NOD will include the trust service provider (QTSP) onto the Trust Service List (TSL).

(Elementi certifikata) Na certifikatu o skladnosti, ki ga izda BV, so navedene naslednje informacije (ki sicer ne spremenijo morebitnih drugih zakonodajnih določb):
- identifikacija in lokacija(e) organizacije;
- identifikacija storitev zaupanja, ki so predmet certificiranja

(Certificate elements) The certificate of conformity issued by BV states the following information (which does not change any other legislative provisions):
- identification and location(s) of the organization;
- identification of the trust services which are subject to certification

- identifikacija relevantnih (e) politik (e) za storitev zaupanja
- uporabljena certifikacijska shema;
- datumi veljavnosti certifikata (datum izdaje in datum veljavnosti);
- referenčni podatki družbe BV, ki je izdajateljica certifikata.

- identification of the relevant policy (policies) for the trust service
- used certification scheme;
- dates of certificate validity (date of its issuance and date of its validity);
- reference data on BV as the certificate issuer.

(Prekinitev formalnega postopka) Po preteku dvanajstih mesecev od prejema zahtevka v primeru, da organizacija morda tudi po opravljenih več presojah za certifikacijo ali dodatnih presojah, ne more dokazati skladnost z zahtevami, se formalni postopki za pridobitev certifikata prekinejo, pogodba s to organizacijo pa se razveljavi. Če certifikat ni izdan, se organizaciji posreduje ustrezna utemeljitev zavrnitve, v kateri je naveden tudi minimalni časovni rok, ki mora preteči, preden se zahtevek lahko ponovno predloži v obravnavo.

(Termination of the formal procedure) If the organization cannot prove conformity with the requirements even after several completed certification audits or additional audits, after the expiry of twelve months from the receipt of the application formal procedures for certificate acquisition shall be terminated and the agreement with this organization shall be annulled. If a certificate has not been issued, the organization shall be provided with an appropriate explanation of the rejection, stating the minimum time period which shall lapse before another application may be submitted for review.

(Podaljšanje ali skrajšanje veljavnosti certifikata) Pri posamezni uporabi certifikata lahko na posebno zahtevo organizacije v obdobju njegove veljavnosti pride do podaljšanja ali skrajšanja veljavnosti certifikata. Za odobritev oziroma zavrnitev tovrstnega zahtevka je pristojna BV, pri čemer bo upošteval morebitne dopolnitve pogodbe in potrebo po dodatni presoji , ki bo lahko opravljeno v kombinaciji z že načrtovano presojo oziroma se bo izvedlo ločeno.

(Extension or shortening of certificate validity) With each individual use of the certificate, its validity can be extended or shortened on special request by the relevant organization filed during the period of its validity. The entity competent to grant or reject such requests is BV, in doing so, it shall take into account any potential amendments to the agreement and need for additional audit, which may be done either in combination with an already planned audit or separately.

(Dodatne presoje) Ponudnik storitev zaupanja mora na osnovi Uredbe (EU) št. 910/2014 člena 24.2.a obvestiti nadzorni organ o vsaki spremembi pri zagotavljanju svojih kvalificiranih storitev zaupanja ter o nameri o prenehanju opravljanja teh dejavnosti. Prav tako mora Ponudnik storitev zaupanja na osnovi ETSI EN 319 403 V2.2.2 točka 7.10 pisno obvestiti BV o vsaki nameravani spremembi pred njeno uveljavitvijo v praksi. Obveščanje mora potekati na elektronski naslov eidas-slovenia@bureauveritas.com. Celotna re–certifikacijska presoja bo izvedena v primerih ko:

(a) je izvedena večja sprememba v obsegu
(b) je izvedena večja sprememba v storitvi zaupanja, ki je v obsegu
(c) je v obseg dodana nova storitev zaupanja
(d) je izvedena večja sprememba v IT sistemu ali poslovnih procesih ponudnika storitev zaupanja) se večji del storitev zaupanja preseli na drugo lokacijo.

V vseh ostalih primerih bo izvedena kontrolna presoja.
Po oceni BV se lahko na sedežu organizacije v naslednjih primerih izvedejo tudi druge vrste dodatnih presoj pri:

(Additional audits) Pursuant to Regulation (EU) No. 910/2014, Article 24.2.a, the trust service provider shall inform the NOD of any change in the provision of its qualified trust services, as well as of its intention to stop performing these activities. Pursuant to ETSI EN 319 403 V2.2.2 point 7.10, the trust service provider shall also inform BV in writing of any intended change before such a change is implemented in practice. The related notifications shall be done via e-mail to the address eidas-slovenia@bureauveritas.com. A full re-certification audit shall be done in the following cases:

(a) if there has been a large change in the scope
(b) if there has been a large change in the trust service included in the scope
(c) if a new trust service has been included in the scope
(d) if there has been a large change in the IT system or business processes of the trust service provider or a major part of the services has been moved to a different location.

In all other cases, surveillance audit shall be performed.
In the opinion of BV, other types of additional audits can also be performed at the organization's headquarters in the following cases:

(a) nepravilni uporabi logotipov;
(b) reklamacijah zaradi situacij, ki bi lahko negativno vplivale na podobo BV;
(c) preverjanju ukrepanja pri ugotovljenih večjih neskladjih (follow-up);
(d) zahtevah, ki bi se pokazale v procesu odobritve certificiranja;
(e) pri odpravi začasne prekinitve veljavnosti certifikata;
(f) pri prejemu obvestila o večjih ali hudih nesrečah oziroma nesrečah s smrtnim izidom in/ali morebitnih kazenskih pregonih/hujših nepravilnostih ali opozorilih, povezanih s certificiranim sistemom;
(g) pri spreminjanju storitve zaupanja organizacije in urejenosti delovanja organizacije;
(h) pri zahtevi nadzornega organa na podlagi Uredbe (EU) št. 910/2014 ali nacionalne zakonodaje;
(i) pri drugih specifičnih zahtevah nadzornih organov.

Morebitna neskladja (NC) je treba ustrezno zabeležiti in jih obravnavati kot pri prvem certificiranju.

(Obnovitev certifikata) Certifikat je do preteka veljavnosti mogoče obnoviti v skladu z pogodbenimi določili. Obnovitev se izvede na podlagi recertifikacijske presoje , ki se izvede enako kot certifikacijska presoja, pri kateri se preveri izpolnitev vseh zahtev.

Formalne postopke za obnovitev certifikata je treba izvesti v obstoječem certifikacijskem ciklu, pravočasno (vsaj 90 dni pred iztekom veljavnosti certifikata), s tem se zainteresirani organizaciji omogoči dovolj dolgo časovno obdobje za odpravo morebitnih neskladij.

(Veljavnost certifikata) Certifikat je veljaven dve leti. Certifikacijski cikel začne teči z dnem sprejetja odločitve o izdaji certifikata oziroma z dnem preteka veljavnosti prejšnjega certifikata, pri re-certifikacijski presoji, pod pogoji, navedenimi v prejšnjem odstavku. Organizacije, ki po preteku veljavnosti certifikata niso izvedle postopkov, potrebnih za obnovitev veljavnosti certifikata, izgubijo pravico do uporabe logotipa/razpoznavnega znaka BV in do izjave, da so njihove dejavnosti certificirane.

7. DRUGE REGULATIVNE DOLOČBE

(Register certificiranih podjetij) Seznam certificiranih organizacij, ki se hrani na sedežu družbe BV je zainteresiranim strankam dostopen na zahtevo.

(Obvezno poročanje) BV periodično obvešča Slovensko akreditacijo o stanju veljavnosti izdanih certifikatov.

(a) incorrect use of logos;
(b) complaints due to situations which could have a negative impact on the image of BV;
(c) checking of measures in the case of established major non-conformities (follow-up);
(d) new requirements which would arise during the process of certification approval;
(e) when eliminating certificate suspensions;
(f) when notification is received about major or severe accidents or accidents with fatalities and/or potential criminal prosecution or severe irregularities or warnings related to the certified system;
(g) in the case of changes in the organization's trust service or orderly functioning of the organization;
(h) in the case of supervisory body's request pursuant to Regulation (EU) No. 910/2014 or national legislation;
(i) in the case of other specific requirements of the supervisory bodies.

Any non-conformity (NC) shall be appropriately recorded and handled as during the first certification.

(Certificate renewal) Each certificate may be renewed before its expiration in accordance with the contractual provisions. Such renewal shall be done on the basis of a re-certification audit which is conducted in the same way as a certification audit, whereby the conformity with all requirements is checked.

Formal procedures for certificate renewal shall be performed within the existing certification cycle and on time (at least 90 days before the certificate expiry). This gives the interested organization a long enough time period to eliminate any non-conformity.

(Certificate validity) Each certificate shall be valid for two years. The certification cycle shall begin on the day when the decision on certificate issuance is adopted or on the day when the previous certificate expires in the case of a re-certification audit under the conditions stated in the previous paragraph. Those organizations which did not perform the procedures necessary to renew the certificate's validity after its expiry shall forfeit their right to use the logo/distinctive mark of BV or to make statements that their activities are certified.

7. OTHER REGULATORY PROVISIONS

(Register of certified companies) A list of certified organizations which is kept at the headquarters of BV is available to interested parties on request.

(Compulsory reporting) BV periodically informs the Slovene Accreditation on the validity of issued certificates.

(Prenos certifikata) Pred prenosom certifikata je potrebno izvesti ponovno analizo celotnega poslovanja (pregled poročil vsaj na zadnji dve leti) certifikacijskega organa naslednika, (transfer) presoja centralnega sedeža ponudnika storitev zaupanja (TSP), ki mora trajati vsaj dva delovna dneva, in (transfer) presoja v enem delovnem dnevu za vsako lokacijo, na kateri se izvajajo dejavnosti povezne s storitvijo zaupanja. Pri prenosu certifikata organizacij v katerih so bila v zadnjih dveh letih izdana neskladja z vidika neizpolnjevanja certifikacijskih zadev, mora (transfer) presoja ponudnika storitev zaupanja (TSP) trajati vsaj toliko časa, kolikor bi trajala glede na izračun števila presojevalskih dni za novo organizacijo, njen cilj pa mora biti potrditev uspešnosti sprejetih korektivnih ukrepov.

(Začasna prekinitev veljavnosti certifikata) BV si pridržuje pravico do začasne prekinitve veljavnosti certifikata, če:

(a) bi na kontrolni presoji bile ugotovljene neskladnosti, ki bi huje in s takojšnjimi posledicami vplivale na značilnosti certificiranih storitev/izdelkov;

(b) stranka pri neskladnostih, ugotovljenih pri kontrolnih presojah, v predpisanem času ne bi udejanjila zahtevanih korektivnih ukrepov;

(c) bi prišlo do reklamacij, pravnih postopkov ali neobveščanja v zvezi z upravnimi ali sodnimi ukrepi;

(d) stranka ne bi dovolila izvedbe kontrolnih presoj ali dodatnih presoj v predvidenih rokih, ki jih zahteva certifikacijski organ;

(e) stranka ne bi pravočasno obvestila BV o bistvenih spremembah, ki bi zadevale organizacijo poslovanja družbe ali specifične lastnosti izdelka;

(f) bi stranka nepravilno in zavajajoče uporabljala certifikat BV;

(g) BV ne bi mogla izvesti kontrolno presojo, kot je predvideno kar bi pomenilo neizpolnitev obveznosti, ki bi temeljila na neizvedenem plačilu certifikacije;

(h) bi stranka formalno zahtevala začasno prekinitev veljavnosti.

O začasni prekinitvi odloča in ustrezen sklep sprejme vodja certifikacijskega organa, ki navede tudi začetek, trajanje (ki ne sme presegati 3 mesece), specifično zadevo, na katero se prekinitev nanaša (prekinitev lahko zadeva tudi le en sam del področja uporabe), in pogoje, pod katerimi bo lahko veljavnost certifikata obnovljena. Obdobje začasne prekinitve veljavnosti certifikata ne vpliva na njegovo veljavnost. V obdobju začasne prekinitve veljavnosti certifikata organizacija ne sme uporabljati logotipa/prepoznavnega znaka, prav tako pa ga ne sme uporabljati pri oglaševanju in mora o tem v roku 3 dni obvestiti NOD.

(Certificate transfer) Before transfer of a certificate, a repeat analysis of the overall business operations has to be done (review of reports at least for the past two years) relating to the successor certifying body, (transfer) audit of the trust service provider (TSP)'s central headquarters at least two business days in duration, and (transfer) audit done for one business day for each location, at which activities related to trust services are performed. In the case of transfer of the certificate for organizations in which non-conformity was established in the past two years from the viewpoint of failure to meet certification matters, such (transfer) audit of the trust service provider (TSP) shall last at least as long as it would otherwise last based on the calculation of audit days for a new organization, and its goal should be to confirm the success of the adopted corrective actions.

(Certificate suspension) BV reserves the right to suspend a certificate if:

(a) a non-conformity is established during surveillance audit which affects the characteristics of certified products/services severely and with immediate consequences;

(b) in the case of a non-conformity established during surveillance audits, the Client does not implement the required corrective actions within the prescribed time;

(c) there are any complaints, legal procedures or failure to notify related to administrative or judicial measures;

(d) the Client does not allow the performance of surveillance audits or additional audits within the prescribed time limits as required by the certification body;

(e) the Client does not inform BV on time of any significant changes relating to the organization of the company's business operations or any specific product properties;

(f) the Client uses the BV certificate in an incorrect or misleading manner;

(g) BV is unable to perform surveillance as planned, which constitutes failure to fulfil its obligations based on non-payment of certification;

(h) the Client formally requests certificate suspension.

Decisions on certificate suspension shall be made and an appropriate decision shall be passed by the director of the certification body, who shall also determine the beginning, duration (not exceeding 3 months), specific matter to which the suspension relates (suspension may also refer to a single area of use), and the conditions under which certificate validity may be renewed. The period of certificate suspension shall not affect its validity. During the period of certificate suspension, the organization shall not use the logo/distinctive mark; it shall also not use it for any advertising and shall inform the NOD thereof within 3 days.

Certificirana stranka mora torej izvesti vsa potrebna dejanja za obnovitev skladnosti s certifikacijskimi zahtevami in o tem mora obvestiti BV, ki si – na stroške stranke – pridržuje pravico, da izvede dodatno presojo.

(Preklic certifikata) BV lahko izdani certifikat prekliče, če:
(a) v predvidenih časovnih rokih niso bili odpravljeni vzroki, ki so privedli do začasne prekinitve veljavnosti certifikata;
(b) nastanejo izjemno velike neskladnosti, ki ne ogrožajo le kakovostnih lastnosti in varnosti uporabe certificiranega izdelka/storitve, temveč tudi samo podobo BV;
(c) se ne izvedejo ukrepi za zagotavljanje skladnosti z zahtevami, predpisanimi za pridobitev certifikacije, v časovnih rokih, ki jih posreduje BV.

Odločitev o preklicu, o katerem sklepa vodja certifikacijskega organa BV, začne veljati z dnem izdaje obvestila o sklepu.
Ob prejemu tovrstnega obvestila bo morala organizacija poskrbeti za uničenje certifikata in mora o tem v roku 3 dni obvestiti NOD.

(Odpoved certifikata) Stranka se lahko odpove certifikatu:
(a) ob izteku obdobja, kot ga določa pogodba, pri čemer mora o odpovedi družbo obvestiti ustrezno in skladno z določili Splošnih pogojev storitev BV;
(b) če ne sprejme rezultatov opravljene presoje in pravilnika družbe BV v zvezi s certificiranjem ali certifikacijskih zahtev;
(c) ob prenehanju opravljanja dejavnosti.

Odpoved začne veljati z dnem izdaje ustreznega obvestila in organizacija mora o tem v roku 3 dni obvestiti NOD.

(Učinki preklica in odpovedi) Ob preklicu in odpovedi certifikata BV poskrbi za izbris imena stranke iz svojega registra in za umik certifikata, o čemer obvesti, če bi bilo to potrebno, tudi ustrezne upravne organe.

Stranka se zaveže, da bo izvirni certifikat uničila, da ne bo uporabljala njegovih kopij in da bo iz tehnične in oglasne dokumentacije izbrisala vsakršno referenco ali simbol, ki bi se skliceval na preklican certifikat in da bo o tem v roku 3 dni obvestila NOD.
Ti pogoji začnejo veljati tudi pri certifikatih, ki niso bili obnovljeni, ko je pretekla njihova veljavnost.

(Uporaba certifikata in logotipa/prepoznavnega znaka BV) Po pridobitvi certifikata se lahko organizacija v svoji

The certified party shall therefore perform all of the necessary actions to restore conformity with the certification requirements and shall inform BV thereof. BV reserves the right to perform an additional audit, at the Client's cost.

(Certificate revocation) BV may revoke an issued certificate if:
(a) the reasons which led to certificate suspension have not been remedied within the stated time limits;
(b) extremely large non-conformity occurs that does not only threaten the quality properties and safety of use of the certified product/service, but the very image of BV;
(c) actions for ensuring conformity with the prescribed requirements for obtaining the certificate have not been implemented within the time limits set by BV.

The decision on certificate revocation which is passed by the director of the BV certification body shall come into force on the day when the notification thereof is issued.
Upon receipt of such notification, the organization shall make sure that the certificate is destroyed and shall inform the NOD thereof within 3 days.

(Certificate waiver) The Client may waive a certificate:
(a) upon expiry of the period determined in the agreement. The company shall be appropriately informed of the waiver, in accordance with the provisions of the General Terms and Conditions of BV Services;
(b) if it does not accept the results of completed audit and the rules of BV related to certification or certification requirements;
(c) upon the termination of its business activities.

Such waiver shall come into force on the day when an appropriate notification is issued and the organization shall notify the NOD thereof within 3 days.

(Effects of revocation and waiver) Upon any revocation or waiver of a certificate, BV shall make sure that the Client's name is deleted from its register and the certificate is withdrawn, when necessary also notifying the relevant authorities.
The Client hereby undertakes to destroy the original certificate, not to use any copies thereof and to delete from its technical and advertising documentation any reference or symbol that would refer to the revoked certificate, as well as to inform the NOD thereof within 3 day .
The said terms and conditions shall also begin to apply for certificates which were not renewed after the expiry of their validity.

(Use of the certificate and logo/distinctive mark of BV) Having acquired a certificate, the organization may

dokumentaciji in pri svojem obveščanju dosledno sklicuje na pridobljeni certifikat ob upoštevanju področja uporabe, za katerega je certifikat pridobila, pri tem pa ne sme podajati dvoumnih informacij, zavajajočih vsebin ali diskreditirati BV.
BV organizacijo poleg tega pooblašča za uporabo lastnega prepoznavnega znaka, skladno z navodili za uporabo certifikacijskih oznak BV, povezanih z uporabljeno shemo. Organizacija pa se mora o načinih uporabe certifikata in/ali prepoznavnega znaka vsekakor predhodno posvetovati z BV, to pa stori tako, da ji pošlje osnutke uporabe, skladno s podrobnimi navodili, ki jih organizaciji posreduje BV. Logotip/oznako lahko organizacija začne uporabljati šele potem, ko tudi NOD odobri ponudniku storitev zaupanja (TSP) status kvalificiranega ponudnika storitev zaupanja (QTSP).

(Reklamacije in prizivi) BV redno pregleduje in obravnava reklamacije in prizive zainteresiranih strani, reklamacije in prizive, povezane s storitvami BV ter reklamacije in prizive, povezane s storitvami, ki jih za druge uporabnike izvajajo stranke BV.
R~~Postopek r~~eševanje reklamacij ~~in prizivov~~ poteka v skladu z operativnim postopkom ~~BV internim postopkom~~ OP 8.2-02 Reševanje reklamacij, obravnavanje prizivov pa po internem predpisu ~~ki je organizaciji dostopen na zahtevo ter v primeru "Obravnavanje prizivov"~~ IP 8.2-01 Obravnavanje prizivov. Oba dokumenta sta strankam na razpolago na zahtevo.
Reklamacijo ali priziv se lahko vloži tudi preko internetne strani: https://www.bureauveritas.si/mnenje-strank-pritozbe-prizivi

SPREJETJE/ODOBRITEV
S podpisom organizacija sprejema vse navedeno v teh splošnih pravilih, ki so sestavni del pogodbenega odnosa organizacije in BV, ki sta ga obe pogodbeni strani sprejeli/potrdili za izvedbo certificiranja.

_____
[datum]

_____
[za organizacijo]

consistently refer to the acquired certificate in its documentation and all its communications, taking into account the area of its use for which such a certificate was acquired. No ambiguous information or misleading contents may be provided and BV shall not be discredited in any way. Furthermore, BV also authorizes the organization to use its own distinctive mark, in line with rules for the use of the BV certification marks associated with the used scheme. However, the organization shall definitely consult BV in advance regarding the ways of using the certificate and/or the distinctive mark. This can be done by sending drafts of their use to BV, in accordance with detailed instructions provided to the organization by BV. The organization may start using the logo/mark only after the NOD has also approved the qualified trust service provider (QTSP) status for the trust service provider (TSP).

(Complaints and appeals) BV regularly reviews and handles complaints and appeals filed by interested parties, complaints and appeals related to BV services, and complaints and appeals related to services provided to other users by the clients of BV.
The procedure for resolving complaints ~~and appeals~~ is conducted in accordance with operational procedure~~the BV Internal Procedure~~ OP 8.2-02 "Resolving of Complaints"~~,~~ while appeals are handled as per internal rule ~~which is available to the organization on request and in the case of "Handling of Appeals"~~ IP 8.2-01 Handling of Appeals.

Complaints and appeals may be filed via the following website too: https://www.bureauveritas.si/mnenje-strank-pritozbe-prizivi

ACCEPTANCE/APPROVAL
By signing these Rules, the organization accepts all of the above statements in these General Rules which are an integral part of the contractual relationship between the organization and BV, and which both Parties have accepted/approved for the implementation of certification.

_____
[Date]

_____
[On behalf of the organization]