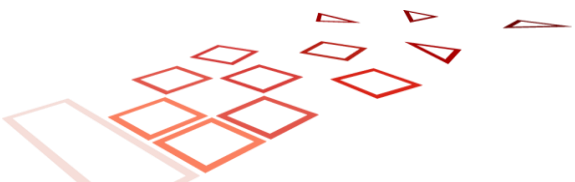
ARDACO
DATA & COMMUNICATION SECURITY

Pravidlá na výkon SSAS Ardaco

ver. 1.0.1

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	1.2.2026	Richard Margala	Prvá verzia dokumentu.
1.0.1	16.2.2026	Richard Margala	Oprava kapitoly Obchodné podmienky



Obsah

1 Úvod

Tento dokument definuje pravidlá na výkon pre poskytovateľa služieb podpisovania serverových aplikácií (Server Signing Application Service Provider, SSASP) Ardaco, a.s, so sídlom. Polianky 5, 841 01 Bratislava, zapísanej v Obchodnom registri Okresného súdu Bratislava I, v oddiely Sa, vložka číslo 2903/B (ďalej aj ,,Ardaco" alebo ,,Poskytovateľ"), ktorý implementuje, presadzuje a aktualizuje vyhlásenie o praxi Služieb podpisovania serverových aplikácií (Server Signing Application Service, SSAS), ktoré je vyhlásením o praxi dôveryhodných služieb podľa definície v norme ETSI EN 319 401, vytvorené pre SSAS.

Základný rámec pre poskytovanie kvalifikovaných dôveryhodných služieb tvoria:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (nariadenie eIDAS)
- Zákon č. 272/2016 Z.z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR
- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2024/1183 z 11. apríla 2024, ktorým sa mení nariadenie (EÚ) č. 910/2014, pokiaľ ide o zriadenie európskeho rámca digitálnej identity

2 Kontaktné údaje

Adresa sídla spoločnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovenská republika
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail pre nahlasovanie incidentov:	incidents@adraco.com

3 Skratky

CA	Certificate Authority	Certifikačná autorita
CID	Commission Implementing Decision	Vykonávacie rozhodnutie Komisie
DTBS/R	Data To Be Signed Representation	Reprezentácia údajov, ktoré majú byť podpísané
eID	electronic IDentification	Elektronická Identifikácia
EUDI wallet	European Digital Identity wallet	Európska peňaženka digitálnej identity
EUSPv2	EU SSAS Policy	Politika EÚ SSAS
HSM	Hardware Security Module	Hardwarový bezpečnostný modul
OID	Object IDentifier	Identifikátor objektu
PIN	Personal Identification Number	Osobné identifikačné číslo
QSCD	Qualified electronic Signature/Seal Creation Device	Kvalifikované zariadenie na vytvorenie elektronického podpisu/pečate
SAD	Signature Activation Data	Údaje na aktiváciu podpisu
SAM	Signature Activation Module	Aktivačný modul podpisu
SAP	Signature Activation Protocol	Protokol podpisu
SCDev	Signature Creation Device	Zariadenie na vytvorenie podpisu

SP	SSAS Policy	Politika SSAS
SSAS	Server Signing Application Service	Služba serverovej podpisovej aplikácie
SSASP	Server Signing Application Service Provider	Poskytovateľ služby serverovej podpisovej aplikácie
TSP	Trust Service Provider	Poskytovateľ dôveryhodných služieb
URI	Uniform Resource Identifier	Jednotný identifikátor zdroja

4 Všeobecný koncept

Daný dokument pokrýva:
SSAS practice statement (Vyhlásenie o praxi SSAS, SSASPS)
Vyhlásenie o praxi SSAS opisuje, ako SSASP prevádzkuje svoju službu, a je vo vlastníctve SSASP. SSASPS je prispôsobená organizačnej štruktúre, prevádzkovým postupom, zariadeniam a prostrediu poskytovateľa dôveryhodných služieb (TSP). Príjemcami SSASPS sú audítori, subscribers (predplatitelia) a relying parties (spoliehajúce sa strany).

SSAS Policy (Politika SSAS, SP)
SSAS Policy (SP) opisuje, čo je cieľom pre určenie uplatniteľnosť služby SSAS. SP je definovaná nezávisle od konkrétnych detailov prevádzkového prostredia poskytovateľa služby SSAS (SSASP). Príjemcami SSASPS sú audítori, subscribers (predplatitelia) a relying parties (spoliehajúce sa strany).

5 General provisions on practice statement and policies

5.1 Názov dokumentu a jednoznačná identifikácia

Názov dokumentu (jednoznačná identifikácia)	Pravidlá na výkon SSAS Ardaco v 1.0.1
OID	0.4.0.19431.1.1.4 itu-t(0) identified-organization(4) – ICO 35829036 etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4) S účinnosťou od 31. marca 2025 musia certifikáty obsahovať OID politiky EUSPv2.

Akákoľvek zmena SP zabezpečí aj zmenu identifikátora danej politiky.

5.2 Účastníci

5.2.1 SSASP

Poskytovateľ – subjekt zodpovedný za poskytovanie SSAS. Poskytovateľ môže vykonávaním časti služieb poveriť iný subjekt (napr. registračnú autoritu), avšak nesie zodpovednosť za dodržanie požiadaviek a opatrení, ktoré sú predmetom tejto politiky.

Základné informácie o vydávajúcej CA:

Sériové číslo:	7ff729b79fdb1cb1bda611af098ecc33d9b18ecf
Algoritmus podpisu:	sha256RSA
DN vydavateľa	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
DN držiteľa	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
Číslo záznamu v dôveryhodnom zozname	TLISK-133

5.2.2 Zákazník a Držiteľ

V rámci týchto zásad môže byť Zákazníkom (Signer) priradený k podpisovému kľúču:

- fyzická osoba;
- fyzická osoba identifikovaná v spojení s právnickou osobou;
- právnická osoba (ktorou môže byť organizácia, jednotka alebo oddelenie identifikované v spojení s organizáciou); alebo
- zariadenie alebo systém prevádzkovaný fyzickou alebo právnickou osobou alebo v mene fyzickej alebo právnickej osoby.

Držiteľ (Subscriber) - Fyzická osoba alebo právnická osoba, ktorej je vydaný Certifikát a ktorá je právne viazaná Zmluvou s predplatiteľom alebo Podmienkami používania.

Zákazník je fyzická alebo právnická osoba, ktorej Poskytovateľ poskytuje Dôveryhodné služby na základe Zmluvy.

Držiteľ je osoba uvedená v kvalifikovanom certifikáte ako držiteľ súkromného kľúča patriacemu k verejnému kľúču, ktorý je uvedený v danom certifikáte.

Zákazník a Držiteľ (ďalej Subjekt) môžu byť dve rôzne entity. Zákazník môže byť napr. organizácia, ktorá využíva služby Poskytovateľa na zabezpečenie certifikátov pre fyzické osoby - Držiteľov, ktoré sú s touto organizáciou v určitom vzťahu (zamestnanci, konatelia a pod). Povinnosti Držiteľa a Zákazníka sú uvedené v Zmluve o vydaní a používaní kvalifikovaného certifikátu.

5.2.3 Spoliehajúce sa strany

Spoliehajúcimi stranami sú subjekty spoliehajúce sa pri svojej činnosti na výstupy poskytovania Dôveryhodných služieb podľa tejto CPS.

6 Pravidlá pre TSP

6.1 Zverejňovanie informácií a úložiská

Dokumentácia k SSAS je schvaľovaná a upravovaná v súlade s definovaným procesom „GL-450-Control of Documents“ vrátane zodpovedností za udržiavanie dokumentácie ako aj ich aktualizáciu. Aktualizácia SSAS dokumentácie je vykonávaná minimálne raz za rok a v prípade akejkoľvek zmeny. V prípade zmeny nevyžadujúcej opätovné overenie externou adítorskou spoločnosťou, je dokument publikovaný do 14 dní od schválenia zmeny.

Všetky zmeny SSASPS a SP či zmluvných podmienok musia byť a budú publikované aj na webovom sídle (viď položka „Internetová adresa“ v kapitole 2 Kontaktné údaje.

Oznamovanie dôležitých zmien v poskytovaní dôveryhodnej služby príslušným stranám v súlade s obchodnými požiadavkami a príslušnými zákonmi a predpismi, vrátane zmien v poskytovaní dôveryhodných služieb a zámeru ukončiť jej poskytovanie bude publikované na webovom sídle „Internetová adresa“ v kapitole 2 Kontaktné údaje. Taktiež bude postupované na základe Plánu ukončenia činností. Všetky relevantné ako aj spoliehajúce sa strany v predstihu budú informované podľa požiadaviek zákona

Informácie o certifikáte sa zverejňujú v súlade s Ardaco CPS - https://www.qsign.sk/doc/ardaco_tsp_cps.pdf

Spoločnosť Ardaco sprístupňuje svoj repozitár verejne iba na čítanie. Sú implementované logické a fyzické bezpečnostné opatrenia, ktoré zabraňujú neoprávneným osobám pridávať, mazať alebo upravovať položky repozitára.

Dokumentácia k SSAS byť dostupné 24 hodín denne, 7 dní v týždni. V prípade zlyhania systému, služby alebo iných faktorov, ktoré nie sú pod kontrolou poskytovateľa služieb zabezpečenia dát (TSP), vynaloží TSP maximálne úsilie, aby zabezpečil, že táto informačná služba nebude nedostupná dlhšie ako maximálny čas uvedený v DR Pláne.

6.2 Inicializácia kľúčového páru

6.2.1 Generovanie podpisového kľúča

Podpisové kľúče sú generované kryptografickým modulom SCDev skladajúcim sa s modulu SAM a HSM.

- Modul SAM spĺňa úroveň EAL4+ rozšírenú o ALC_FLR.2 a AVA_VAN.5 podľa normy ISO/IEC 15408. Modul zároveň spĺňa požiadavky normy CEN EN 419 241-2
- Modul HSM je spolu so SAM certifikované ako QSCD zariadenie. Modul spĺňa požiadavky Protection Profile podľa normy CEN EN 419 221-5

Použité kryptografické algoritmy sú v súlade s požiadavkami definovanými štandardizačnými orgánmi ETSI/TS 113 312 a SOG-IS-CRYPTO.

Podpisový kľúč Signer-a sa generuje pred vygenerovaním certifikátu, ale ako súčasť procesu generovania certifikátu.

TSP podporuje nasledujúce kryptografické algoritmy a dĺžky kľúčov:

• Kryptografický algoritmus: RSA
• Dĺžka kľúča: 4048 bitov
• Hašovací algoritmus: SHA256

Parametre algoritmu na vytvorenie podpisu sú vybrané tak, aby boli aktuálne odolné a zostali odolné počas celej životnosti certifikátu subjektu.

Súkromné kľúče sú uložené šifrovaným spôsobom v databáze mimo QSCD, čím sa zabezpečuje dôvernosť a integrita.

Viď kapitola 6.1 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.2.2 Prostriedky elektronickej identifikácie alebo prepojenie identity

SSASP poskytuje podpisujúcemu mobilnú aplikáciu ako prostriedok elektronickej identifikácie po úspešnej registrácii.

Prostriedok elektronickej identifikácie obsahuje interný odkaz. Tento odkaz sa používa na zabezpečenie toho, aby identifikačné údaje osoby prepojené s prostriedkom eID boli rovnaké ako údaje prepojené so Subjektom priradeného Certifikátu. eID tiež vytvára jedinečné prepojenie so súkromným kľúčom Podpisujúceho.

Používateľ je oboznámený s podmienkami použitia
Používateľ je oboznámený s preventívnymi bezpečnostnými opatreniami, ktoré musí dodržiavať
Pri registrácii je získaný email, ktorý používateľ potvrdí zo svojej mailovej schránky

Aktivácia aplikácie QSign Mobile ako prostriedku pre elektronickú identifikáciu

1. Používateľ si nastaví aplikačný PIN kód. PIN kód bude vyžadovaný pre každý prístup do aplikácie
2. Používateľ sa prihlási do svojho účtu pomocou mena a hesla
3. Používateľ aktivuje aplikáciu niektorým zo spôsobov:
    a. Pomocou NFC eID
    b. Inou už aktivovanou aplikáciou QSign Mobile
    c. Pomocou operátora
4. Pri aktivácii sa generuje autorizačný kľúč, slúžiaci na autorizáciu operácie podpísania
    a. Kľúč sa generuje v bezpečnom úložisku mobilného zariadenia (Secure Enclave, Strong Box, Tee)
    b. Počas aktivácie sa registruje verejná časť kľúča v SSA, kde je previazaná s konkrétnou aplikáciou a konkrétnym používateľom
    c. Prístup ku kľúču je chránený pomocou screen lock na danom zariadení

SSAS zabezpečuje, aby autorizácia každej podpisovej operácie bola realizovaná pomocou kryptograficky silného mechanizmu založeného na princípe výzva-odpoveď, ktorý je viazaný na konkrétnu transakciu a poskytuje primeranú ochranu proti neoprávnenému použitiu, opakovaniu alebo manipulácii komunikácie.

6.2.3 Prepojenie certifikátov

Prepojenie medzi podpisovým kľúčom a certifikátom nastáva pri vydaní certifikátu, kedy je verejný kľúč podpisového kľúčového páru spojený s certifikátom.
Prepojenie medzi privátnym a verejným kľúčom je zabezpečené kryptograficky. Integrita prepojenia je chránená a podpisujúci nemôže použiť podpisový kľúč predtým, ako sa prepojí certifikát verejného kľúča.

6.2.4 Poskytovanie prostriedkov elektronickej identifikácie

Viď kapitola **Chyba! Nenašiel sa žiaden zdroj odkazov.** Prostriedky elektronickej identifikácie alebo prepojenie identity

6.3 Prevádzkové požiadavky na životný cyklus podpisového kľúča

6.3.1 Aktivácia podpisu

SSASP vyžaduje úspešnú identifikáciu a autentifikáciu podpisovateľa pred povolením akýchkoľvek akcií, ktoré môžu ovplyvniť výhradnú kontrolu nad akýmkoľvek podpisovým kľúčom.
Subjektu je povinný postupovať podľa krokov v kapitole **Chyba! Nenašiel sa žiaden zdroj odkazov.** Prostriedky elektronickej identifikácie alebo prepojenie identity
SSASP poskytuje ochranu podpisových údajov počas prenosu, čím zabezpečuje dôvernosť aj integritu.
QSCD zabezpečuje výhradnú kontrolu podpisujúceho nad podpisovým kľúčom. Zabezpečuje integritu a dôvernosť podpisového kľúča a prepojenie medzi podpisujúcim a podpisovým kľúčom. DTBS sa podpisujú iba podpisovým kľúčom patriacim podpisujúcemu.
Podpisujúci pomocou mobilnej aplikácie komunikuje s SSAS, aby odoslal údaje na aktiváciu podpisu (SAD). SAD spája autentifikáciu podpisujúceho s podpisovým kľúčom a údajmi, ktoré sa majú podpísať, t. j. DTBS/R.
Služba vyžaduje, aby Podpisovateľ poskytol SAD prostredníctvom protokolu aktivácie podpisu (SAP) na overenie, aby sa aktivoval podpisový kľúč.
Služba implementuje opatrenia založené na posúdení rizika na ochranu pred hrozbami pre SAD.
QSCD zabezpečuje, že aktivovaný podpisový kľúč možno použiť iba na podpísanie DTBS/R prijatého ako súčasť protokolu aktivácie podpisu.
Platnosť certifikátu verejného kľúča sa overí pred použitím zodpovedajúceho podpisového kľúča.
Podpisovateľ potvrdí akciu podpisu v mobilnej aplikácii pomocou biometrického overenia alebo overenia PIN kódom zariadenia.

6.3.2 Mazanie podpisového kľúča

Viď kapitola 4.9 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

SSASP zničí súkromný kľúč, ak:
• Platnosť certifikátu prepojeného so súkromným kľúčom vyprší; alebo
• Subjekt požiada o vymazanie účtu a sú splnené zákonné požiadavky.

Prepojenie medzi podpisovým kľúčom a podpisovateľom sa zachová aj po operáciách podpisovania.

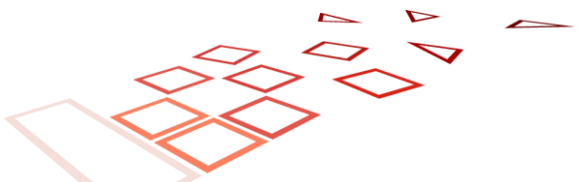
6.3.3 Záloha a obnovenie podpisového kľúča

Viď kapitola 4.8 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.4 Opatrenia fyzickej bezpečnosti, riadenia a prevádzky

6.4.1 Všeobecné

Viď kapitola 5.1, 5.2, 5.3 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.



OVR-6.4.1-01: The requirements identified in ETSI EN 319 401 [1], clauses 5, 6.3 and 7.3 shall apply

6.4.2 Opatrenia fyzickej bezpečnosti

Viď kapitola 5.4 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.4.3 Procedurálne opatrenia

Viď kapitola 5.5 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.4.4 Personálne opatrenia

Viď kapitola 5.6 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.
Viď kapitola 7.2 v Politika Ardaco.

6.4.5 Postup pre uchovávanie auditných záznamov

Viď kapitola 5.7 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.
Viď kapitola 7.10 v Politika Ardaco.

Všetky bezpečnostné udalosti sa zaznamenávajú vrátane zmien týkajúcich sa bezpečnostnej politiky, spustenia a vypnutia systému, zlyhaní systému a zlyhaní hardvéru, aktivít brány firewall a smerovača a pokusov o prístup k systému SSAS.

6.4.6 Archivácia záznamov

Viď kapitola 5.8 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

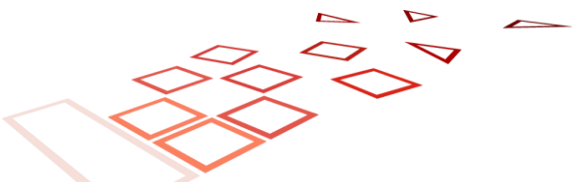
SSASP uchováva záznamy najmenej sedem rokov po skončení platnosti akéhokoľvek certifikátu založeného na týchto záznamoch a v rámci obmedzení platných právnych predpisov.

6.4.7 Výmena kľúčov

Viď kapitola 5.9 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.4.8 Kompromitácia a obnova po havárii

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [1], clauses 7.9 and 7.11 shall apply.
Viď kapitola 5.10 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.
Viď kapitola 7.1 v Politika Ardaco.



6.4.9 SSASP Ukončenie činností

Viď kapitola 4.11 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.
Viď kapitola 7.12 v Politika Ardaco.

6.5 Technické bezpečnostné kontroly

6.5.1 Systémy a riadenie bezpečnosti

Viď kapitola 1.5 a 5 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.5.2 Systémy a prevádzka

Viď kapitola 7.4 v Politika Ardaco.
Viď kapitola 5.7 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.5.3 Počítačové bezpečnostné opatrenia

Viď kapitola 7.4 v Politika Ardaco.

6.5.4 Bezpečnostné opatrenia počas životného cyklu

Viď kapitola 6.3.2 a 7.7 v Politika Ardaco.

6.5.5 Opatrenia sieťovej bezpečnosti

Viď kapitola 6.7 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.6 Audit súladu a ďalšie hodnotenia

Viď kapitola 8 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

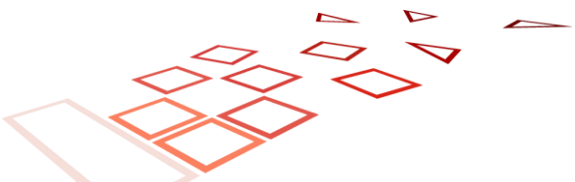
6.7 Iné obchodné a právne záležitosti

6.7.1 Poplatky

Viď kapitola 9.1 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.2 Finančná zodpovednosť

Viď kapitola 9.2 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.



6.7.3 Dôvernosť obchodných informácií

Viď kapitola 9.3 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.4 Ochrana osobných údajov

Viď kapitola 9.4 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.5 Práva duševného vlastníctva

Viď kapitola 9.5 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.6 Vyhlásenia a záruky

Viď kapitola 9.6 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

SSASP je zodpovedný za súlad s postupmi predpísanými v tejto politike, a to aj v prípade, že funkčnosť SSASP vykonávajú externí dodávatelia.

6.7.7 Odmietnutie záruk

Viď kapitola 9.7 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.8 Obmedzenie zodpovednosti

Viď kapitola 9.8 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.9 Náhrada škody

Viď kapitola 9.9 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.10 Podmienky a ukončenie

Viď kapitola 9.10 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.11 Jednotlivé oznámenia a komunikácia s účastníkmi

Viď kapitola 9.11 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.12 Novelizácia

Viď kapitola 9.12 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.13 Riešenie sporov

Viď kapitola 9.13 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.14 Rozhodné právo

Viď kapitola 9.14 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.15 Súlad s platnými právnymi predpismi

Viď kapitola 9.15 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.7.16 Rôzne ustanovenia

Viď kapitola 9.16 v Pravidlá na výkon certifikačných činností (CPS) Ardaco.

6.8 Ostatné ustanovenia

6.8.1 Organizácia

TSP plne zabezpečuje dodržiavanie pravidiel definovaných v dokumente Politika Ardaco publikovanej na verejnom webovom sídle, čo zabezpečuje dodržiavanie pravidiel definovaných v ETSI EN 319 401, klauzula 7.1.

6.8.2 Dodatočné testovanie

Uplatňujú sa požiadavky uvedené v dokumente Pravidlá na výkon certifikačných činností (CPS) Ardaco kapitola 9.17

6.8.3 Obmedzenia

Neuplatňujú sa žiadne obmedzenia.

Poskytované dôveryhodné služby a produkty koncových používateľov používané pri poskytovaní týchto služieb musia byť sprístupnené osobám so zdravotným postihnutím, ak je to možné. V prístupnej a udržateľnej miere sú dodržiavané pravidlá ETSI EN 301 549.

6.8.4 Obchodné podmienky

Viď kapitola 6.2 v Politika Ardaco.

7 Referencie

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R091

[2] Zákon č. 272/2016 Z. z. v znení neskorších predpisov o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

[3] Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu v1.4 - https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf

[4] ISO/IEC 27002:2013 Information Security Management standard, https://www.praxiom.com/iso-27002.htm

[5] ETSI EN 319 401 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);General Policy Requirements for Trust Service Providers, https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf

[6] ETSI EN 319 411-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements - https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[7] ETSI EN 319 411-2 V2.1.1 (2016-02): 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, https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.01.01_60/en_31941102v020101p.pdf

[8] ETSI EN 319 412-1 V1.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, https://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

[9] RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc5280

[10] ITU-T X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[11] CA/Browser Forum (V1.3.0): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf

[12] CEN EN 419241-2:2019: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

[13] ETSI TS 119 431-1 V1.3.1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev

-