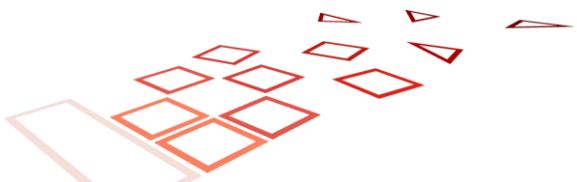
ARDACO
DATA & COMMUNICATION SECURITY

Certifikační politika Ardaco pro služby vyhotovování a ověřování kvalifikovaných certifikátů

v 2.1

Historie změn

Verze	Datum vydání	Schválený	Poznámka
1.0	19.2.2021	Richard Margala	První verze dokumentu.
2.0	12.10.2021	Richard Margala	Začlenění komentářů
2.0.1	16.12.2021	Richard Margala	Oprava terminologických chyb (kapitola 6.1 Zkratky)
2.0.2	30.5.2023	Richard Margala	Začlenění připomínek k auditu a změna Okresního soudu
2.0.3	23.11.2023	Richard Margala	Změna pojmu „Okresní soud Bratislava III“ na „Městský soud Bratislava III“
2.1	12.06.2025	Richard Margala	Doplněna podpora pro kvalifikované certifikáty webových sídel. Odstraněna zmínka o povinnosti předávat vydané certifikáty a CRL NBÚ SR (novelizace právního předpisu).



1 Úvod

Tento dokument definuje certifikační politiku (CP) společnosti Ardaco, a.s., se sídlem. Polianky 5, 841 01 Bratislava, zapsaná v obchodním rejstříku Městského soudu Bratislava III, v oddíle Sa vložte číslo 2903/B (dále jen "Ardaco" nebo "Poskytovatel") důvěryhodné služby, jak je definována v kapitole 1.1

Základní rámec pro poskytování kvalifikovaných služeb vytvářejících důvěru tvoří:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (nařízení eIDAS)
- zákon č. 272/2016 Sb. ze dne 20. září 2016 o službách vytvářejících důvěru pro elektronické obchody na vnitřním trhu a o změně některých zákonů (zákon o službách vytvářejících důvěru)
- Systém dohledu nad kvalifikovanými službami vytvářejícími důvěru definovaný orgánem dohledu – NBU SR
- Zákon č 69 z 30. leden 2018 o kybernetickej bezpečnosti a o změne a doplnení niektorých zákonov
- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

1.1 Přehled

Tato CP definuje vyhotovování a správu certifikátů veřejných klíčů podle X.509 verze 3 [10] v souladu s požadavky dokumentu RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (Internet X.509 Public Key Infrastructure Certificate Revocation List (CRL) Profile) [9], základní požadavky na vydávání a správu veřejně důvěryhodných certifikátů [11] a požadavky nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES ("nařízení eIDAS") [1].

Tyto zásady jsou strukturovány v souladu s RFC 3647 [15].

Tato CP podporuje certifikační autoritu pro následující služby:

- Kvalifikovaná důvěryhodná služba pro vyhotovování a ověřování kvalifikovaných certifikátů pro elektronický podpis
- Kvalifikovaná důvěryhodná služba pro vyhotovování a ověřování kvalifikovaných certifikátů pro elektronickou pečeť
- Kvalifikovanou důvěryhodnou službu vyhotovování a ověřování kvalifikovaných certifikátů pro autentifikaci webových sídel.

Plnění CP KCA NBU při vydávání a ověřování kvalifikovaných certifikátů je dle 5.2.1 SD čl. 17 odst. 5, čl. 24, 28, 38 a 45 nařízení (EU) č. 910/2014. Postup pro plnění požadavků národní legislativy je specifikován zejména v kapitole 10 certifikační politiky kořenového certifikačního úřadu NBA (CP KCA NBU) OID (1.3.158.36061701.0.0.1.2.2), který profiluje ETSI EN 319 411-2 V2.1.1 (2016-02) [8] certifikační politiky pro vydávání kvalifikovaných certifikátů.

Pro poskytování kvalifikované důvěryhodné služby pro vyhotovování kvalifikovaných elektronických časových razítek platí podmínky stanovené v dokumentu, „Certifikačná politika kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných elektronických časových pečiatok” a postupy v dokumentu "Politika Ardaco" pro služby vyhotovování a ověřování kvalifikovaných osvědčení".

1.2 Název dokumentu a jedinečná identifikace

Název dokumentu (jedinečná identifikace)	Certifikační politika pro vydávání a ověřování kvalifikovaných certifikátů ver. 2.0.2
OID	1.3.158. 35829036.0.0.0.0.1 Popis použitého identifikátoru objektu (OID): 1.3. – Organizace identifikovaná podle ISO 1.3.158 - IČO 1.3.158. 35829036. – Ardaco, a.s. 1.3.158. 35829036.0.0.0.0.– CA Ardaco, a.s. 1.3.158. 35829036.0.0.0.1 – CP CA Ardaco, a.s

1.3 Účastníci infrastruktury veřejných klíčů

1.3.1 Certifikační autorita (CA)

Poskytovatel – subjekt odpovědný za poskytování důvěryhodných služeb podle této certifikační politiky. Poskytovatel může pověřit výkonem části Služeb jiný subjekt (např. registrační autoritu), odpovídá však za dodržování požadavků a opatření podléhajících těmto Zásadám.

Hierarchii certifikační autority a autority časových razítek tvoří kořenová certifikační autorita, která je zároveň vydávající certifikačním autoritou pro kvalifikované certifikáty a razítka. Vydávající certifikační autorita také vydá certifikát pro kvalifikovanou službu časových razítek a certifikát potvrzující existenci a platnost certifikátu (OCSP).

Základní informace o vystavující certifikační autoritě:

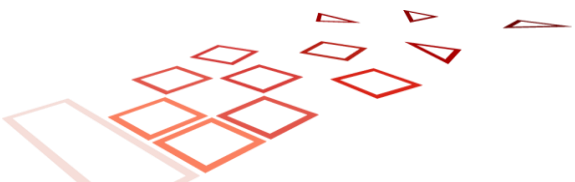
Sériové číslo:	7ff729b79fdb1cb1bda611af098ecc33d9b18ecf
Podpisový algoritmus:	sha256RSA
DN vydavatele	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
DN držáku	C = SK O = Ardaco a.s. 2.5.4.97 = NTRSK-35829036 CN = Ardaco QSCA
Číslo seznamu důvěryhodných položek	TLISK-133

1.3.2 Registrační autorita (RA)

Služby poskytované registrační autoritou jsou poskytovány přímo Poskytovatelem nebo externím smluvním partnerem.

Služby registrační autority obvykle zahrnují:

a) příjem žádostí o certifikát
b) ověření totožnosti žadatele a další údaje, pokud jsou požadovány pro druh certifikátu
c) předání certifikátu držiteli
d) přijímání žádostí o zrušení



RA může své činnosti delegovat na jiného smluvního partnera, ale daný smluvní partner musí splňovat stejné požadavky jako samotná RA. RA je povinna informovat Poskytovatele, o jaký subjekt se jedná, prokázat smluvní dokumentaci a také informovat o každé změně na úrovni smluvního vztahu spolupráce mezi RA a smluvním partnerem.

RA podle smluvních podmínek může:

1. provozovat část technického řešení autentizace uživatelů na vlastních systémech, přičemž v takovém případě musí být zajištěno dodržování bezpečnostní politiky provozovatele,
2. používat vlastní interní procesy a postupy (např. definice a výkon disciplinárního řízení nebo řízení lidských zdrojů), ale i v tomto případě musí být zaručeno dodržování bezpečnostní politiky a procesů správce, jakož i komunikace změn v souvisejících procesech a postupech,
3. jmenovat zaměstnance, kteří důvěřují rolím určeným k výkonu činností RA, a zároveň zajišťují výkon definovaný v kapitole 5.6 Personální opatření.

1.3.3 Zákazník a držitel

Zákazník je fyzická nebo právnická osoba, které Poskytovatel poskytuje Důvěryhodné služby na základě Smlouvy.

Držitelem je osoba uvedená v kvalifikovaném certifikátu jako držitel soukromého klíče patřícího k veřejnému klíči uvedenému v tomto certifikátu.

Držitel KC může být:

a) fyzická osoba
b) fyzická osoba identifikovaná společně s právnickou osobou,
c) právnická osoba, kterou může být organizace nebo její jednotka nebo oddělení,
d) zařízení nebo systém provozovaný fyzickou nebo právnickou osobou nebo jejím jménem;

Zákazník a držitel mohou být dvě různé entity. Zákazníkem může být například organizace, která využívá služeb Poskytovatele k poskytování certifikátů fyzickým osobám – Držitelům, kteří jsou s touto organizací v určitém vztahu (zaměstnanci, vedoucí pracovníci apod.). Povinnosti Držitele a Zákazníka jsou uvedeny ve Smlouvě o vydávání a používání kvalifikovaného certifikátu.

Vztah mezi Zákazníkem a Držitelem může být následující:

a) Při podání žádosti o KC fyzické osoby (Držitele) je Zákazníkem
    1. fyzická osoba sama,
    2. právnická osoba oprávněná zastupovat fyzickou osobu (Držitel), nebo
    3. jakýkoli subjekt, s nímž je fyzická osoba (držitel) spojena, např. právnická osoba, která ho zaměstnává, nezisková organizace, jejímž je členem atd.).
b) Při podání žádosti o KC pro právnickou osobu je Zákazníkem
    1. jakýkoli subjekt, který je podle příslušného právního systému oprávněn zastupovat právnickou osobu, nebo
    2. statutární orgán právnické osoby žádající o její dceřiné společnosti nebo jednotky nebo útvary.
c) Při poptávce KC pro zařízení nebo systém provozovaný fyzickou nebo právnickou osobou je Zákazníkem:
    1. fyzická nebo právnická osoba provozující zařízení nebo systém,
    2. jakýkoli subjekt, který je podle platných právních předpisů oprávněn zastupovat právnickou osobu, nebo
    3. statutární orgán právnické osoby žádající o její dceřiné společnosti nebo jednotky nebo útvary.

1.3.4 Spoléhající se strany

Spoléhající se strany jsou subjekty, které při svých činnostech spoléhají na výstupy poskytování služeb vytvářejících důvěru podle této CP.

1.3.5 Bezpečnostní rada

Bezpečnostní rada (dále jen "Rada") přijímá důležitá opatření v oblasti bezpečnosti. Rada zahrnuje alespoň tyto úlohy:

- Security Officer
- Information Security Officer
- System Auditor

Bezpečnostní rada se schází nejméně jednou za 6 měsíců, aby posoudila bezpečnostní situaci a provedla nezbytné změny bezpečnostních postupů.

Rada má konečnou pravomoc a odpovědnost specifikovat a schvalovat certifikační politiky, samotný CPS, jakož i zajistit, aby certifikační politiky byly přezkoumávány s cílem udržovat je aktuální.

Členy správní rady jmenuje a jmenuje provozní ředitel.

1.3.6 Ostatní účastníci

Účast dalších účastníků je definována platnou legislativou (Orgán Dohledu, orgány činné v trestním řízení apod.).

Poskytovatel cloudových služeb disponuje vlastní optickou sítí a poskytuje technologický prostor pro klientská zařízení ve 3 datových centrech a je držitelem certifikátu ISO27001:2014 pro poskytování služeb v oblasti telekomunikací, informačních technologií a služeb datových center.

1.4 Použití certifikátů

Kvalifikované certifikáty lze používat pouze v souladu s platnými právními předpisy. Kvalifikovaný certifikát podle tohoto CP může být vydán pro:

- fyzickou osobu za účelem podpory zdokonaleného elektronického podpisu dle čl. 2. 26 a 27 Nařízení eIDAS [QCP-n]
- právnickou osobu za účelem podpory zdokonalená elektronická razítka dle čl. 2. 36 a 37 Nařízení eIDAS [QCP-l]
- fyzickou osobu, kde soukromý klíč se nachází na zařízení pro vyhotovení kvalifikovaného elektronického podpisu/razítka, za účelem podpory kvalifikovaného elektronického podpisu dle čl. 3 bod 12 Nařízení eIDAS [QCP-n-qscd]
- právnickou osobu, kde soukromý klíč se nachází na zařízení na vyhotovení kvalifikovaného elektronického podpisu/pečetě, za účelem podpory kvalifikovaná elektronická razítka podle čl. 3 bod 27 Nařízení eIDAS [QCP-l-qscd]
- fyzickú alebo právnickú osobu za účelom autentifikácie webových sídiel podľa čl. 3 bod 38 a čl. 45 Nariadenia eIDAS [QEVCP-w]

1.5 Správa politiky

1.5.1 Kontaktní údaje

Tabulka obsahuje údaje Poskytovatele, který je zodpovědný za přípravu, tvorbu a údržbu tohoto dokumentu.

Adresa sídla společnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovensko
	Společnost je zapsána v obchodním rejstříku Městského soudu Bratislava III, oddíl Sa, vložka č. 2903/B.
IČ	35 829036
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com

1.5.2 Kontaktní osoba

Pro účely tvorby politiky zřídil Poskytovatel samostatný orgán pro řízení politiky (Bezpečnostní rada), který je plně odpovědný za její obsah a který je připraven zodpovědět veškeré dotazy týkající se politiky Poskytovatele.

Tabulka obsahuje kontaktní údaje na složku zodpovědnou za provoz certifikačních autorit Poskytovatele.

Adresa sídla společnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovensko
	Společnost je zapsána v obchodním rejstříku Městského soudu Bratislava III, oddíl Sa, vložka č. 2903/B.
IČ	35 829036
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail s hlášením incidentů:	incidents@ardaco.com
Telefonní číslo:	+421 2 3221 2311

1.5.3 Postup komunikace

Dotknuté osoby: Zákazník, spoléhající se strany, dodavatelé a další třetí strany.
Dotknuté CA: CA Ardaco, a.s. a všechny podřízené certifikační autority vydané tímto kořenovým certifikačním úřadem

V případě podezření, že přišlo v souvislosti s certifikáty vydanými výše uvedenou certifikační autoritou:
ke kompromitaci soukromého klíče
neoprávněné vydání osvědčení
jiný případ podvodu nebo
jakýkoli jiný případ nevhodného chování

Pro nahlášení incidentů je nutné takový nález nahlásit na e-mail incidents@adraco.com či info@ardaco.com nebo volejte **+421 2 3221 2311**

1.5.4 Osoba rozhodující o souladu CPS s CP

Osobou odpovědnou za rozhodování o souladu postupů Poskytovatele uvedených v CPS s touto CP je Bezpečnostní rada jmenovaná vedením.

1.5.5 CPS a postupy schvalování vnějších politik

Ještě před zahájením provozu musí mít Poskytovatel schválenou CP a příslušnou CPS a musí splnit všechny jeho požadavky. Obsah CP a CPS je schvalován osobami jmenovanými do Bezpečnostní rady (viz kapitola 1.5.5).

1.6 Definice a zkratky

1.6.1 Zkratky

CA	Certifikační autorita
CP	Certifikační politika
CPS	Pravidla pro výkon certifikačních činností
CRL	Seznam odvolaných certifikátů
ČP	Časové razítko
KC	Kvalifikovaný certifikát
PKI	Infrastruktura veřejných klíčů
RA	Registrační autorita
QSCD	Zařízení na vyhotovení kvalifikovaného elektronického podpisu (Qualified Signature Creation Device)

1.6.2 Definice

Definice podle Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické traNBUkce na vnitřním trhu a o zrušení směrnice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R091 [1]:

1. "elektronickou identifikací" proces používání osobních identifikačních údajů v elektronické podobě, které jedinečně reprezentují fyzickou nebo právnickou osobu nebo fyzickou osobu zastupující právnickou osobu;
2. "prostředkem pro elektronickou identifikaci" hmotná nebo nehmotná jednotka obsahující osobní identifikační údaje, která se používá k ověření pravosti pro online služby;
3. "osobními identifikačními údaji" soubor údajů umožňujících identifikovat fyzickou nebo právnickou osobu nebo fyzickou osobu zastupující právnickou osobu;

4. "systémem elektronické identifikace" systém elektronické identifikace, v jehož rámci jsou prostředky pro elektronickou identifikaci vydávány fyzickým nebo právnickým osobám nebo fyzickým osobám zastupujícím právnické osoby;
5. "ověřením" elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické nebo právnické osoby nebo původ a integritu údajů v elektronické podobě;
6. "spoléhající se stranou" fyzická nebo právnická osoba, která využívá elektronickou identifikaci nebo službu vytvářející důvěru;
7. "subjektem veřejného sektoru" ústřední, regionální nebo místní orgán, veřejnoprávní subjekt nebo sdružení tvořené jedním nebo více takovými orgány nebo jedním či více veřejnoprávními subjekty nebo soukromoprávní subjekt pověřený poskytováním veřejných služeb alespoň jedním z těchto orgánů, subjektů nebo sdružení, pokud jedná na základě tohoto pověření;
8. „veřejnoprávním subjektem“ je subjekt v smyslu článku 2 ods. 1 bodu 4 směrnice Evropského parlamentu a Rady 2014/24/EÚ;
9. "podepisovatel" fyzická osoba, která vytváří elektronický podpis;
10. "elektronickým podpisem" data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podpisu;
11. "zaručeným elektronickým podpisem" elektronický podpis, který splňuje požadavky stanovené v článku 26;
12. "kvalifikovaným elektronickým podpisem" zaručený elektronický podpis vytvořený pomocí kvalifikovaného prostředku pro vyhotovování elektronických podpisů a založený na kvalifikovaném certifikátu pro elektronické podpisy;
13. "daty pro vyhotovování elektronických podpisů" jedinečná data používaná podepisující osobou pro vyhotovování elektronických podpisů;
14. "certifikátem pro elektronický podpis" elektronické potvrzení, které spojuje data pro ověřování platnosti elektronického podpisu s fyzickou osobou a potvrzuje alespoň jméno nebo pseudonym této osoby;
15. "kvalifikovaným certifikátem pro elektronický podpis" certifikát pro elektronický podpis vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňující požadavky stanovené v příloze I bodě 1;
16. "důvěryhodná služba" elektronická služba obvykle poskytovaná za úplatu, která sestává z: vyhotovování, ověřování a ověřování platnosti elektronických podpisů, elektronických pečetí nebo elektronických časových razítek, služeb elektronického doporučeného doručování a certifikátů souvisejících s těmito službami nebo vyhotovování, ověřování a potvrzování certifikátů pro autentizaci internetových stránek nebo pro ukládání elektronické podpisy, pečetě nebo certifikáty související s těmito službami;
17. "kvalifikovaná důvěryhodná služba " důvěryhodná služba, která splňuje příslušné požadavky stanovené v nařízení [1];
18. „orgán posouzení shody“ je orgán vymezen v článku 2 bode 13 nařízení (ES) č. 765/2008, které je akreditovaný v souladu s nařízením [1] jako způsobilý k posuzování shody kvalifikovaných poskytovatelů důvěryhodných služeb a jimi poskytovaných kvalifikovaných důvěryhodných služeb;
19. "poskytovatelem služeb vytvářejících důvěru" fyzická nebo právnická osoba, která poskytuje jednu nebo více služeb vytvářejících důvěru jako kvalifikovaný nebo nekvalifikovaný poskytovatel služeb vytvářejících důvěru;
20. "kvalifikovaným poskytovatelem služeb vytvářejících důvěru" poskytovatel služeb vytvářejících důvěru, který poskytuje jednu nebo více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele;
21. "produktem" hardware nebo software nebo příslušné součásti hardwaru nebo softwaru, které jsou určeny k použití při poskytování služeb vytvářejících důvěru;
22. "prostředkem pro vyhotovování elektronických podpisů" konfigurovaný software nebo hardware používaný pro vyhotovování elektronických podpisů;

23. "kvalifikovanými prostředky pro vyhotovování elektronických podpisů" prostředek pro vyhotovování elektronických podpisů, který splňuje požadavky stanovené v bodě 1 přílohy II;
24. "tvůrcem pečeti" právnická osoba, která vytváří elektronickou pečeť;
25. "elektronickou pečetí" data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zajistit původ a integritu těchto souvisejících údajů;
26. "zaručení elektronický razítkem" elektronická značka, která splňuje požadavky stanovené v čl. 36 odst. 1;
27. "kvalifikovaným elektronickým razítkem" zaručená elektronická pečeť vytvořená kvalifikovaným prostředkem pro vyhotovování elektronických pečetí a založená na kvalifikovaném certifikátu pro elektronickou pečeť;
28. "daty pro vyhotovování elektronických razítek " jedinečná data, která tvůrce elektronické pečeti používá k vytvoření elektronické pečeti;
29. "certifikátem pro elektronickou značku" elektronické potvrzení, které spojuje data pro ověřování platnosti elektronických pečetí s právnickou osobou a potvrzuje její název;
30. "kvalifikovaným certifikátem pro elektronickou pečeť" certifikát pro elektronickou pečeť vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňující požadavky stanovené v příloze III bodě 1;
31. "prostředkem pro vyhotovování elektronických pečetí" konfigurovaný software nebo hardware používaný k vytvoření elektronické pečetě;
32. "kvalifikovaným prostředkem pro vyhotovování elektronických pečetí" prostředek pro vyhotovování elektronických pečetí, který splňuje obdobně požadavky stanovené v příloze II bodě 1;
33. "elektronickým časovým razítkem" data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým časem, čímž prokazují existenci těchto jiných údajů v daném okamžiku;
34. "kvalifikovaným elektronickým časovým razítkem" elektronické časové razítko, které splňuje požadavky stanovené v článku 42;
35. "elektronickým dokumentem" jakýkoli obsah uložený v elektronické podobě, zejména text nebo zvuková, vizuální nebo audiovizuální nahrávka;
36. "službou elektronického doporučeného doručování" služba, která umožňuje přenos dat mezi třetími stranami elektronickými prostředky a poskytuje důkazy o nakládání s předávanými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo jakýchkoli neoprávněných změn;
37. "kvalifikovanou službou elektronického doporučeného doručování" služba elektronického doporučeného doručování, která splňuje požadavky stanovené v článku 44;
38. "certifikátem pro autentizaci internetových stránek" osvědčení, které umožňuje autentizaci internetových stránek a odkazuje na tyto internetové stránky s fyzickou nebo právnickou osobou, jíž byl certifikát vydán;
39. "kvalifikovaným certifikátem pro autentizaci internetových stránek" certifikát pro autentizaci internetových stránek, který je vydán kvalifikovaným poskytovatelem důvěryhodných služeb a splňuje požadavky stanovené v příloze IV;
40. "daty pro ověřování platnosti" data, která se používají k ověření platnosti elektronického podpisu nebo elektronické značky;
41. "ověřením" proces ověřování a potvrzování platnosti elektronického podpisu nebo elektronické značky

1.6.3 Odkazy

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické traNBUkce na vnitřním trhu a o zrušení směrnice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R091

[2] zákon č. 272/2016 Sb., ve znění pozdějších předpisů, o službách vytvářejících důvěru pro elektronické obchody na vnitřním trhu a o změně některých zákonů (zákon o službách vytvářejících důvěru)
[3] Systém kvalifikovaného dohledu nad službami vytvářejícími důvěru podle definice orgánu dohledu verze 1.4 – https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf
[4] ISO/IEC 27002:2013 Norma pro řízení bezpečnosti informací, https://www.praxiom.com/iso-27002.htm
[5] ETSI EN 319 401 V2.1.1 (2016-02): Elektronické podpisy a infrastruktury (ESI); Obecné požadavky zásad pro poskytovatele služeb vytvářejících důvěru, 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): Elektronické podpisy a infrastruktury (ESI); Zásady a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Všeobecné požadavky - 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): Elektronické podpisy a infrastruktury (ESI); Zásady a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 2: Požadavky na poskytovatele služeb vytvářejících důvěru vydávající kvalifikované certifikáty EU 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), elektronické podpisy a infrastruktury (ESI); profily certifikátů; Část 1: Přehled a běžné datové struktury, 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 Informační technologie - Propojení otevřených systémů - Adresář: Rámce certifikátů veřejného klíče a atributů
[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: Důvěryhodné systémy podporující podepisování serverů – Část 2: Profil ochrany pro QSCD pro podepisování serveru
[13] Politika Ardaco
[14] Certifikační politika pro KC a Certifikační politika pro ČP
[15] RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani et al - https://www.rfc-editor.org/rfc/pdfrfc/rfc3647.txt.pdf
[16] Pravidla pro výkon certifikačních činností (CPS) Ardaco a.s.
[17] Popis řešení Remote QSCD - interní dokument
[18] PSD2: Smernica (EÚ) 2015/2366 Európskeho parlamentu a Rady z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES

2 Zveřejňování informací a archivů

Certifikáty musí být umístěny tak, aby byly přístupné držitelům, zákazníkům a spoléhajícím stranám. Funkci úložiště certifikátů plní webová stránka Poskytovatele, která je veřejně dostupná.

Přístup k informacím o certifikátech certifikačních autorit Poskytovatele je veřejně dostupný bez omezení. Poskytovatel nezveřejní konečné certifikáty Držitelů ve svém sídle bez přímého souhlasu Držitele nebo subjektu, pro který je certifikát vydán, a to za následujících pravidel definovaných a veřejně přístupných v dokumentu Pravidla pro výkon certifikačních činností (CPS) Ardaco a.s.[16]

Dokument CP je schválen a upraven v souladu s definovaným procesem "GL-450-Kontrola dokumentů", včetně odpovědnosti za údržbu CP a jeho aktualizaci.

Veškeré změny CP musí a budou rovněž zveřejněny na webových stránkách (viz bod "Internetová adresa").

3 Identifikace a autentizace

Tato kapitola popisuje:

1. postupy používané k ověření identity nebo jiných atributů žadatele o certifikát koncového uživatele u certifikační autority nebo RA před vydáním certifikátu
2. stanoví postupy pro ověřování totožnosti a kritéria pro přijímání žadatelů subjektů, které se chtějí stát certifikační autoritou, orgánem příslušným k právním přezkumu nebo jinými subjekty působícími v infrastruktuře veřejných klíčů nebo s ní spolupracujícími.
3. Popisuje, jak jsou ověřovány strany požadující opětovné vytvoření klíče nebo odvolání.
4. Popisuje postupy pojmenování, včetně rozpoznávání ochranných známek pro určité názvy

3.1 Typy jmen

Poskytovatel vytvoří certifikáty s rozlišovacími jmény v souladu s platnými technickými normami, zejména odporučením ITU-T X.509 [10] a IETF RFC 5280 [9] a příslušné části ETSI EN 319 412 [8]

3.2 Smysluplnost jmen

Použitá jména musí spolehlivě identifikovat osoby, jimž jsou certifikát vydávána, a musí být snadno srozumitelná. Forma jména vychází z formy běžně používané pro identifikaci osoby (skutečné jméno a příjmení fyzické osoby, název právnické osoby zapsané v příslušném rejstříku, název orgánu veřejné moci).

3.3 Anonymita a používání pseudonymů

Poskytovatel neumožňuje vydání certifikátu anonymní osobě.

Poskytovatel umožňuje vydání certifikátu, ve kterém je místo běžně používaného jména uvedeno jiné jméno. V takovém případě musí v názvu obsahovat také text "PSEUDONYM". Mandátní certifikát podle § 8 odst. 5 zákona č. 272/2013 Sb. nesmí obsahovat pseudonym.

Poskytovatel si vyhrazuje právo odmítnout jméno, které je hanlivé, porušuje obecné slušnosti nebo může uvést spoléhající se stranu v omyl tím, že poskytne nepravdivou a zavádějící představu o tom, kdo je skutečným držitelem.

3.4 Jedinečnost jmen

Poskytovatel garantuje jedinečnost jmen (pole *Subject*) pro všechny vydané certifikáty.

3.5 Uznávání, ověřování a význam ochranných značek

V certifikátu mohou být použity pouze ochranné značky, jejichž vlastnictví nebo pronájem byly žadatelem o certifikát uspokojivě potvrzeny.

Poskytovatel si vyhrazuje právo ochrannou značku v certifikátu nezmiňovat. Poskytovatel nenese odpovědnost za zneužití ochranní značky.

3.6 Počáteční ověření totožnosti

3.6.1 Prokázání vlastnictví soukromého klíče

Pokud není pár klíčů generován Poskytovatelem, je vlastnictví privátního klíče, který odpovídá veřejnému klíči, prokázáno požadavkem ve formátu PKCS#10. Požadavek PKCS#10 je podepsán soukromým klíčem, který prokazuje, že soukromý klíč je v držení žadatele.

Má-li kvalifikovaný certifikát obsahovat atribut, že klíč je umístěn na QSCD, musí být pár klíčů, pro který je kvalifikovaný certifikát vydán, vygenerován přímo na kvalifikovaném prostředku pro vytváření elektronických podpisů (QSCD), které splňuje požadavky nařízení eIDAS. Poskytovatel je povinen tuto skutečnost ověřit.

Společnost se řídí jakož i má definovaný interní proces, definující podrobnosti pro realizaci řešení pro podepisování kvalifikovaným elektronickým podpisem na dálku v rámci výkonu kvalifikovaných důvěryhodných služeb Ardaco, a.s. podle NAŘÍZENÍ KOMISE (EU) 2015/1502 ze dne 8. září 2015, kterým se stanoví minimální technické specifikace a postupy pro úrovně zabezpečení prostředků elektronické identifikace podle či. 10 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1995/2003 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu.

3.6.2 Ověření identity jednotlivce

Poskytovatel musí ověřit identitu fyzické osoby a jakýchkoli specifických atributů, které jsou uváděny v certifikátu podle samostatného volně publikovaného dokumentu Pravidla pro výkon certifikačních činností [16]

3.6.3 Ověření oprávnění jednat

Ověření oprávnění jednat je potřebné pro vydání mandátního certifikátu podle § 8 zákona č. 1/2003. 272/2016 Sb. Ověření oprávnění jednat je definován v samostatném volně publikovaném dokumentu Pravidla pro výkon certifikačních činností [16]

3.6.4 Ověření totožnosti právnické osoby

Poskytovatel musí ověřit identitu právnické osoby a všechny specifické atributy uvedené v certifikátu buď:

a) fyzickou přítomnost zplnomocněného zástupce nebo
b) metody poskytující stejný stupeň záruk jako fyzická přítomnost zplnomocněného zástupce

Ověření totožnosti právnické osoby je definován v samostatném volně publikovaném dokumentu Pravidla pro výkon certifikačních činností [16]

3.6.5 Ověření kontroly nad doménou

Poskytovatel musí ověřit vlastnictví, resp. kontrolu nad doménou v případě, že je v certifikátu uvedena, podle publikovaného dokumentu Pravidla pro výkon certifikačních činností [16].

3.7 Identifikace a autentizace u žádostí o opětovné vydání klíče

Při opětovném vydání klíče (následného certifikátu) Zákazník prokazuje vlastnictví klíče, totožnost a oprávnění způsobem uvedeným v sekci 3.6 Počáteční ověření totožnosti. K podpisu žádosti může použít originál kvalifikovaného certifikát platného v době podání žádosti.

Pokud se některá z podmínek služby změní, změny budou oznámeny účastníkovi a odsouhlaseny v souladu s ustanoveními kapitoly. 4.4.

3.8 Identifikace a autentizace pro žádosti o zrušení platnosti certifikátu

Oprávněnými osobami pro zaslání žádosti o zrušení platnosti certifikátu jsou

a. Držitel certifikátu
b. osoba, jejímž jménem Držitel jedná (typicky zánik oprávnění)
c. státní orgány, které k tomu mají ze zákona oprávnění

Žádost o zrušení platnosti certifikátu lze předložit v listinné nebo elektronické formě. Žádost musí být autentizována, přičemž oprávněný subjekt ji může autentizovat:

a) osobně, po identifikaci způsobem podle sekce 3.6
b) vzdáleně s uvedením autentizačního hesla určeného k tomuto účelu
c) vzdáleně, podpisem žádosti o zrušení certifikátu klíčem, který má být zrušen

Poskytovatel si vyhrazuje právo zrušit po dohodě s oprávněným subjektem certifikát i jiným způsobem, na kterém se dohodnou, a který jednoznačně prokazuje vůli oprávněného subjektu. Platnost certifikátu může být zrušena i Poskytovatelem, oprávněná role je uvedena v provozní směrnici.

Podrobné informace o oprávněných osobách, procesu zneplatnění a jsou uvedeny v sekci 4.9.

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o certifikát

4.1.1 Kdo může požádat o certifikát

Osobami, které jsou oprávněny požádat Poskytovatele o vydání certifikátu, jsou:

a) **kvalifikovaný certifikát** – fyzická osoba pro sebe nebo osoba jí pověřená
b) **kvalifikované pověření –** fyzická osoba po prokázání splnění požadavků dle §8 odst. 3 zákona č. 272/2016 Sb. nebo subjekt, se kterým je tato fyzická osoba ve smyslu daného odstavce propojena.
c) **Kvalifikovaný certifikát pro razítko** – osoba oprávněná jednat jménem právnické osoby nebo pověřená právnickou osobou

d) **Kvalifikovaný certifikát pro autentifikaci webového sídla** - fyzická nebo právnická osoba provozující zařízení resp. systém nebo jakákoli entita (Zákazník), která ve smyslu platné národní legislativy jedná jménem dané právnické osoby,

V případě, že o vydání certifikátu žádá zplnomocněná osoba, musí se prokázat úředně ověřeným zmocněním, které prokazuje oprávněnost zmocněnce provést daný úkon jménem zmocnitele.

4.1.2 Registrační proces a povinnosti

Proces registrace se provádí před počátečním vydáním certifikátu. Proces je iniciován žadatelem.

Registrační proces a povinnosti je definován v samostatném volně publikovaném dokumentu Pravidla pro výkon certifikačních činností [16]

4.2 Zpracování žádosti o certifikát

Po provedení identifikace a autentifikace (3.6 Úvodní ověření identity, 3.7 Identifikace a autentifikace pro žádosti opakované vydání klíče) musí být žádost odeslána Poskytovateli. Registrační údaje musí být přenášeny zabezpečeným kanálem. V případě externí RA musí být údaje přijaty pouze od známých RA, jejichž identita byla ověřena.

4.3 Vydání certifikát

Poskytovatel vydává certifikáty bezpečným způsobem tak, aby byla zajištěna jejich autenticita. Pokud je pár klíčů generován Poskytovatelem, musí zajistit důvěrnost údajů v průběhu celého procesu. Poskytovatel používá software ke kontrole shody se standardem formátu požadavku (PKCS#10).

Během celé existence CA nesmí být stejné rozlišující jméno (distinguished name) v certifikátu použito pro dvě různé entity.

4.4 Převzetí certifikátu

4.4.1 Způsob převzetí

Podrobné podmínky toho, co představuje převzetí certifikát, jsou stanoveny v obchodních podmínkách.

4.4.2 Zveřejnění certifikátu

Certifikát je publikován v souladu s kapitolou 1.6.3. Aplikují se omezení pro zveřejňování osobních údajů.

4.4.3 Oznámení o vydání certifikát jiným stranám

Neuplatňuje se.

4.5 Použití klíčového páru klíčů a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem

Držitel je povinen zejména

a) používat soukromý klíč a certifikát pouze k účelu, ke kterému byl určen
b) dodržovat všechna ustanovení tohoto CPS, Smlouvy o poskytování Služby a legislativy pro důvěryhodné služby, které se vztahují k povinnostem Držitele
c) zabránit neoprávněnému použití soukromého klíče
d) neprodleně informovat Poskytovatele o skutečnostech, které vedou ke zneplatnění certifikátu, především ztrátu, podezření z neoprávněného použití soukromého klíče nebo kompromitaci přístupových údajů
e) při kompromitaci soukromého klíče okamžitě ukončit jeho používání

4.5.2 Použití veřejného klíče a certifikátu Spoléhající se stranou

Spoléhající se strany jsou povinny:

a) používat certifikát pouze k účelu, pro který byl určen
b) ověřit stav certifikátu pomocí aktuálních informací o stavu zrušení, jak jsou zveřejňovány spoléhajícím se stranám
c) dodržovat všechna ustanovení tohoto CPS a právní předpisy o důvěryhodných službách, které se týkají povinností spoléhající se strany

4.6 Obnovení certifikátu

Poskytovatel neposkytuje službu obnovení certifikátu. Obnovením certifikátu se rozumí vydání následného certifikátu k dosud platnému certifikátu beze změny veřejného klíče nebo informací uvedených v certifikátu. Poskytovatel nesmí vydat certifikát veřejnému klíči, ke kterému již byl certifikát v minulosti vydán.

4.7 Vydání navazujícího certifikát

Vydáním následného certifikátu se rozumí vydání nového certifikátu stejného typu a se stejným obsahem pro registrovaného držitele.

4.7.1 Podmínky pro vydání následného certifikát

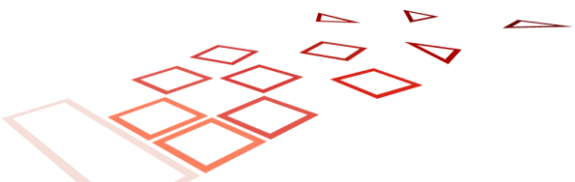
Žádná ustanovení.

4.7.2 Kdo může požádat o následné certifikát

O vydání následného certifikátu může požádat existující Zákazník a/nebo Držitel, který musí splňovat požadavky na identifikaci a autentizaci podle 3.6.

4.7.3 Postup podání žádosti o vydání následného certifikátu

Postup podávání žádostí je totožný s žádostí o počáteční certifikát, kap. 4.1. Poskytovatel je povinen oznámit Objednateli a Držiteli každou změnu podmínek služby a předat mu je ke odsouhlasení.



4.7.4 Oznámení o vydání následného certifikát

Poskytovatel vhodným způsobem informuje Držitele o vydání následného certifikátu.

4.7.5 Přijetí následného certifikát

Použije se postup v kapitole. 4.4.1.

4.7.6 Zveřejnění následného certifikát

Použije se postup v kapitole. 4.4.2

4.7.7 Oznámení o vydání následného certifikát jiným stranám

Použije se postup v kapitole 4.4.3

4.8 Změna certifikátu

Poskytovatel nepodporuje službu modifikace certifikátu (vystavování certifikátu s upraveným obsahem beze změny páru klíčů).

4.9 Zrušení a pozastavení platnosti certifikátu

4.9.1 Podmínky pro odvolání certifikátu

Poskytovatel zruší Certifikát zejména na základě následujících okolností:

a) o zrušení certifikátu požádá oprávněná osoba podle 4.9.2
b) Poskytovatel zjistí, že došlo ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče patřícího k danému certifikátu
c) Poskytovatel zjistí, že při vydání certifikátu nebyly splněny požadavky platné legislativy 272/2016 Sb.
d) Poskytovatel zjistí, že certifikát byl vydán na základě nepravdivých údajů
e) Poskytovatel se dozví podstatnou skutečnost, která znamená, že certifikát nadále nemůže plnit svůj účel např. Držitel zemřel, byl prohlášen za mrtvého, byl zbaven svéprávnosti, organizace uvedená v certifikátu zanikla nebo došlo ke změně údajů, které jsou uvedeny v certifikátu
f) V případech, kdy nastanou skutečnosti uvedené v právních předpisech pro důvěryhodné služby nebo příslušných standardech a normách (např. neplatnost údajů v Certifikátu)

Poskytovatel si vyhrazuje právo akceptovat i další podmínky pro zrušení, které však nesmí být v rozporu s platnými právními předpisy.

Zrušené certifikát nesmí být v žádném případě obnoveno.

4.9.2 Kdo může požádat o odvolání certifikátu

Chcete-li požádat o odvolání certifikátu, předložte:

g) Držitel
h) další osoba uvedená ve smlouvě o poskytování služeb

i) Oprávněné osoby dle § 8 odst. 4. zákona č. 272/2016 Sb. v případě mandátního certifikátu
j) Poskytovatel v souladu s podmínkami 4.9.1
k) další subjekty v souladu s platnou legislativou

4.9.3 Postup při žádosti o zrušení certifikátu

Žádost o zrušení certifikátu lze podat osobně v otevírací době uvedené na internetových stránkách poskytovatele nebo elektronicky na kontaktních adresách uvedených v kapitole A. 0. Poskytovatel zveřejňuje formulář pro odvolání certifikátu na svých webových stránkách.

Žádost musí být ověřena buď:

a) identifikací a autentizací stejným způsobem jako při prvotním ověření totožnosti 3.6
b) identifikací a autentizací technickými prostředky k tomuto účelu určenými
c) prokázání dohodnutých autentizačních údajů pro odvolání certifikátu, které Objednatel/Držitel obdrží při vystavení certifikátu
d) podepsáním žádosti o odvolání certifikátu klíčem, který patří k certifikátu, který má být odvolán

Žádost musí obsahovat jednoznačnou identifikaci certifikátu, který má být zrušen. Jednoznačnou identifikací je pořadové číslo certifikátu, v případě, že není oprávněné osobě známo, může být použito kombinací dalších údajů umožňujících jednoznačnou identifikaci. Datum a čas zneplatnění certifikátu jsou určeny zpracováním žádosti.

Po vyřízení žádosti Poskytovatel informuje Žadatele o výsledku zpracování. V případě ohrožení soukromého klíče nebo hrozby kompromitace musí být žádost podána ihned, tj. jakmile se žadatel dozvěděl o kompromitaci soukromého klíče nebo hrozbě zpronevěry. Poskytovatel neodpovídá za škodu vzniklou v důsledku nedodržením lhůty dle předchozí věty Žadatelem. Poskytovatel neodpovídá za škodu způsobenou užitím Certifikátu v době po podání žádosti o jeho zrušení, pokud dodržel lhůty stanovené v bodech 4.9.4 a 4.9.5.

4.9.4 Doba zpracování žádosti

Maximální doba mezi přijetím žádosti o jeho zneplatnění je 24 hodin. Zrušení nabývá účinku zveřejněním.

4.9.5 Latence publikování seznamu CRL

Poskytovatel zveřejní seznam CRL ihned po jeho vydání. Latence pro publikování je určena výhradně latencí infrastruktury a je zanedbatelná v čase.

4.9.6 Oznámení o zneplatnění certifikátu jiným stranám

Na základě § 6 odst. 2 písm. b) zákona č. 272/2016 Sb. Potvrzení o datu a čase jejich zrušení zašle poskytovatel do 30 dnů od jejich zrušení Národnímu bezpečnostnímu úřadu.

4.10 Služby ověřování stavu certifikátů

Ověření stavu certifikátů vydaných Poskytovatelem je možné na základě CRL nebo OCSP. Seznamy CRL jsou generovány nejméně každých 24 hodin a jsou automaticky publikovány v úložišti (viz kapitola. 1.6.3). Stav certifikátu vydaného Poskytovatelem lze ověřit také pomocí služby OCSP, tato informace je vždy obsažena ve vydaném certifikátu. Pokud byla adresa služby OCSP zahrnuta do certifikátu, znamená to, že tato služba je k dispozici pro daný certifikát.

Služby jsou k dispozici 24 hodin denně, 7 dní v týdnu, přičemž Poskytovatel zaručuje integritu a jedinečnost poskytovaných informací. V případě výpadku systému nebo jiných faktorů nezávislých na vůli Poskytovatele vynaloží Poskytovatel veškeré úsilí, aby doba nedostupnosti nepřesáhla nezbytně nutnou dobu.

Informace o odvolání certifikátu v seznamu CRL a OCSP jsou konzistentní a jsou udržovány v odpovědi seznamu CRL nebo OCSP nejméně do vypršení platnosti certifikátu.

4.11 Ukončení poskytování služeb

Podmínky ukončení poskytování služeb jsou uvedeny v obchodních podmínkách.

4.12 Úschova a obnova klíčů

Poskytovatel tuto službu neposkytuje.

5 Fyzická bezpečnost, řízení a provozní opatření

5.1 Bezpečnostní politika (Information security policy)

Organizace má definovanou politiku bezpečnosti informací jako samostatný dokument, která je schválena vedením organizace, která stanovuje přístup organizace k řízení její informační bezpečnosti.

Změny v politice bezpečnosti informací se v případě potřeby oznamují třetím stranám (předplatitelům, spoléhajícím se stranám, hodnotícím orgánům, dozorčím nebo jiným regulačním orgánům).

Politika bezpečnosti informací je tedy zdokumentována, implementována a udržována včetně bezpečnosti kontroly a provozní postupy pro zařízení, systémy a informační aktiva organizace poskytující důvěryhodné služby. Také je zveřejněna a oznámena všem zaměstnancům, kterých se to týká.

Politika bezpečnosti informací a soupis aktiv pro informační bezpečnost je pravidelně přezkoumávána v plánovaných intervalech nebo dojde-li k významným změnám s cílem zajistit jejich nepřetržitou vhodnost a přiměřenost a efektivnost. Všechny změny, které mají vliv na úroveň poskytované bezpečnosti, jsou schváleny.

Konfigurace systémů je také pravidelně kontrolována na změny, které porušují bezpečnostní politiky.

5.2 Fyzická bezpečnostní opatření

5.2.1 Prostory

Všechny systémy a zařízení pro provoz kvalifikovaných důvěryhodných služeb jsou provozovány v prostorách, které jsou chráněny před neautorizovaným přístupem. Fyzická ochrana prostor spočívá v jasně oddělených bezpečnostních perimetrech (fyzické bariéry – stěny, mříže), přičemž bezpečnostní perimetr není sdílen s jinými organizacemi.

5.2.2 Fyzický přístup

Veškerý přístup do fyzicky zabezpečených prostor podléhá nezávislému dohledu. Ochrana objektu je řešena bezpečnostní službou a elektronickým zabezpečovacím systémem. Přístup neoprávněných osob je možný pouze v doprovodu autorizovaných osob. Každý vstup a výstup z prostor je zaznamenán. Mechanismy používané k autorizaci přístupu jsou popsány v dokumentaci k datovému centru.

5.2.3 Napájení a klimatizace

Napájení je zajištěno několika pobočkami s vlastními transformátory a záložním zdrojem (UPS, generátor). Chlazení je zajištěno redundantními klimatizačními jednotkami.

5.2.4 Ochrana před vodou

Prostory jsou umístěny mimo záplavové území a realizovány tak, aby nemohlo dojít k ohrožení vodou z jiných zdrojů.

5.2.5 Ochrana před ohněm

Prostory jsou odděleny od přímých zdrojů tepla a ohně a jsou chráněny automatickým protipožárním systémem na bázi elektricky nevodivého hasicího média.

5.2.6 Uchovávání médií

Média v elektronické a papírové podobě jsou uložena tak, aby byla chráněna před náhodným nebo úmyslným poškozením a neoprávněným přístupem (kovová skříň, trezor). Záložní kopie se uchovávají v prostorách, které nejsou fyzicky spojeny s provozními prostory.

5.2.7 Nakládání s odpady

Paměťová média obsahující důvěrné informace musí být před smazáním nebo opětovným použitím fyzicky zničena, nebo musí být zničena informace, které obsahují (vymazání a přepis dat namísto jednoduchého vymazání/formátování). Postupy jsou podrobně upraveny vnitřní směrnicí.

Nakládání s odpady nesmí poškozovat životní prostředí.

5.3 Procesní opatření

5.3.1 Důvěryhodné role

Poskytovatel zaměstnává zaměstnance nebo subdodavatele, kteří mají potřebné odborné znalosti, spolehlivost, zkušenosti a kvalifikaci a kteří prošli školením o pravidlech bezpečnosti a ochrany soukromí odpovídajících nabízeným službám a pracovní funkci. Zaměstnanci jsou formálně jmenováni do důvěryhodných rolí vedením společnosti. Pro každou roli jsou definovány kvalifikační požadavky, rozsah odpovědnosti a kompatibilita příslušné role s ostatními rolemi. Provozní postupy pro každou roli, včetně požadavků na dvojí řízení pro jejich provádění, jsou definovány v interní dokumentaci. Jejich výkonnost je kontrolována interním auditem.

Pro provoz jsou definovány následující základní role:

- **Security Officer:** celková odpovědnost za navrhování, zavádění, zlepšování a monitorování bezpečnostních postupů.
- **Information Security Officer:** návrh, implementace, zlepšování a monitorování informační bezpečnosti a řízení rizik IT.
- **System Administrator**: instalace, konfigurace a údržba TSP důvěryhodných systémů.
- **System Operator:** provoz důvěryhodných TSP systémů na denní bázi, včetně zálohování.
- **System Auditor:** provádění interních auditů, shromažďování a vyhodnocování důkazů o souladu provozu TSP s platnou legislativou CP, CPS a interními politikami a směrnicemi. Oprávnění k prohlížení archivů a auditních záznamů důvěryhodných systémů TSP.
- **RA Operator:** zajišťuje registraci a ověření totožnosti Zákazníků a Držitelů a informací obsažených v certifikátu, schvaluje žádosti o vydání a zneplatnění certifikátu.

5.3.2 Počet osob vyžadován na výkon činností

Zabezpečeno v souladu s interními provozními postupy.

5.3.3 Identifikace a autentizace

Pro činnosti zahrnující manipulaci s TSP zařízeními včetně obnovy jejich zálohy se používají čipové karty, pro registrační činnosti zas bezpečné jméno a heslo.

5.3.4 Nekompatibilita rolí

Zabezpečeno v souladu s interními provozními postupy.

5.4 Personální opatření

Zaměstnanci v důvěryhodných rolích jsou jmenováni formálním jmenováním vedením a jsou prokazatelně poučeni o popisu práce, povinnostech, odpovědnostech a pracovních postupech.

5.4.1 Požadavky na kvalifikaci, praxi a povolení

Kvalifikační požadavky pro jednotlivé role jsou uvedeny v interní provozní směrnici a jsou používány při výběrových řízeních.

Personál i schválení subdodavatelé disponují s potřebnou odborností, spolehlivostí, zkušenostmi, kvalifikací a vhodnou odbornou přípravou týkající se předpisů v oblasti bezpečnosti a ochrany osobních údajů a uplatňuje administrativní a řídící postupy, které odpovídají evropským nebo mezinárodním normám.

5.4.2 Postupy detekční kontroly

Pracovníci v důvěryhodných rolích jsou prověřeni personálním oddělením na základě poskytnutých referencí a nemohou být odsouzeni za úmyslný trestný čin.

5.4.3 Požadavky na školení personálu

Pracovníci v důvěryhodných rolích jsou při jmenování proškolováni a následně pravidelně rekvalifikováni v tématech relevantních pro výkon jejich činnosti (min. 1x ročně). Školení zahrnuje informace o nových bezpečnostních hrozbách a postupech.

5.4.4 Požadavky, rekvalifikace personálu a jejich četnost

Viz kap. 5.4.3

5.4.5 Frekvence a posloupnost otáčení válce

Řídí se vnitřními organizačními pravidly Poskytovatele.

5.4.6 Sankce za nepovolené činnosti

Řídí se vnitřními organizačními pravidly Poskytovatele podle stupně závažnosti přestupku.

5.4.7 Dokumentace, kterou musí poskytnout zaměstnanci

Pro výkon každé funkce je zaměstnancům prokazatelně poskytována dokumentace v nezbytném rozsahu (viz 5.4). Pracovníci jsou povinni používat dokumenty pouze k určenému účelu.

5.5 Auditní stopy

Poskytovatel eviduje a uchovává po přiměřenou dobu, a to i po ukončení činnosti TSP, veškeré relevantní informace týkající se vydaných a přijatých údajů, zejména pro účely poskytnutí důkazů v soudním řízení a pro účely zajištění kontinuity služby.

5.5.1 Typy protokolovaných událostí

Poskytovatel zaznamenává různé typy událostí, což je detailně definováno v samostatném volně publikovaném dokumentu Pravidla pro výkon certifikačních činností [16].

5.5.2 Frekvence zpracování záznamů

Záznamy jsou zpracovávány s frekvencí závislou na jejich charakteru dle interní směrnice.

5.5.3 Doba uchovávání

Záznamy o auditu jsou uchovávány v aktivní podobě minimálně 1 rok, v případě záznamů týkajících se životního cyklu certifikátů minimálně 1 rok po skončení jejich platnosti. Následně jsou přesunuty do archivu s dobou archivace dle kap.5.6.2

5.5.4 Ochrana auditních stop

Elektronické auditní záznamy jsou chráněny způsobem, který zaručuje jejich integritu a pravost (kombinace HW a SW opatření, WORM, elektronický podpis) a jsou pravidelně zálohovány.

Listinné auditní záznamy jsou zpracovávány a uchovávány tak, aby nedošlo k jejich ztrátě, poškození nebo zničení.

5.5.5 Postupy pro zálohování záznamů auditu

Auditní záznamy jsou zálohovány v souladu s vnitřní směrnicí a platnou legislativou Slovenské republiky.

5.5.6 Systém pro sběr záznamů o auditu

Sběr listinných auditních záznamů probíhá manuálně. Sběr elektronických auditních záznamů, které generují přímo systémy a zařízení TSP infrastruktury je automatizovaný, ostatní elektronické auditní záznamy jsou sbírány manuálně.

5.5.7 Oznámení subjektu, který událost způsobil

Neuplatňuje se.

5.5.8 Posouzení zranitelnosti

Uplatňují se požadavky stanovené v bodě 7.7 písm. g) bodě ii), bodě 7.8 písm. g), bodě 7.9 písm. h) a bodu 7.11 normy ETSI EN 319 401 [5], které jsou definovány v samostatném dokumentu Politika pro KC a certifikační politika pro KC a ČP.

5.6 Uchovávání záznamů

Záznamy jsou uchovávány ve formě, ve které byly vytvořeny (papírové nebo elektronické) nebo v převedené podobě s využitím zaručené konverze dle zákona č. 305/2013 Sb. Záznamy musí být uchovávány takovým způsobem, aby nemohly být poškozeny nebo ztraceny.

5.6.1 Typy archivovaných záznamů

Poskytovatel archivuje záznamy minimálně v následujícím rozsahu:

- záznamy podle 5.5.1
- vydány certifikáty
- seznamy zrušených certifikátů
- oficiální korespondence
- bezpečnostní dokumentace
- instalační média

5.6.2 Doba uchovávání

Podle § 5 zákona č. 272/2016 Sb. Z.z.je doba archivace min. 10 let.

5.6.3 Ochrana archivů

Archivní záznamy jsou chráněny před negativními vlivy prostředí, jako je vlhkost, teplota, v případě elektronických archiválií magnetismus, pokud to jejich technologie vyžaduje. Záznamy jsou chráněny kombinací přístupových a režimových opatření.

5.6.4 Postupy zálohování

Postupy zálohování archivu jsou navrženy tak, aby umožňovaly úplné obnovení. Podrobnosti jsou stanoveny ve vnitřní směrnici.

5.6.5 Požadavky na přidávání časových razítek

Neuplatňuje se.

5.6.6 Systém sběru archivů

Neuplatňuje se.

5.6.7 Postupy pro získávání a ověřování archivních informací

Neuplatňuje se.

5.7 Výměna klíčů

Výměna klíčů se provádí:

- před vypršením platnosti certifikátu CA minimálně 30 dní, ale optimálně 1 rok předem
- v případě ohrožení zabezpečení nebo důvodného podezření na ohrožení soukromého klíče certifikační autority

Při informování účastníků a hlášení bezpečnostních incidentů se dodržují příslušná ustanovení CP, CPS a vnitřních pokynů.

5.8 Zotavení po kompromitace a havárii

V případě kompromitace nebo havárii se poskytovatel řídí interním plánem obnovy a řešení incidentů, který rovněž popisuje mechanismy informování dotčených stran a orgánu dohledu.

5.8.1 Postupy pro řešení incidentů a ohrožení

Postupy pro řešení incidentů a kompromitace jsou upraveny interními směrnicemi. Postupy jsou testovány, přezkoumávány a aktualizovány nejméně 1x ročně. Společnost zajistí, aby byl nahlášený incident zaznamenán do 48 hodin nebo v souladu s platnými zákony.

5.8.2 Postupy při poškození výpočetních zdrojů, softwaru a/nebo dat

Použijí se ustanovení této kapitoly. 5.8.1.

5.8.3 Postupy pro ohrožení soukromého klíče

Použijí se ustanovení této kapitoly. 5.8.1.

5.8.4 Kontinuita podnikání po katastrofě

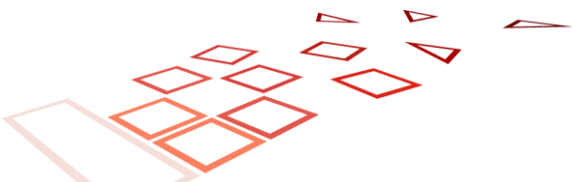
Použijí se ustanovení této kapitoly. 5.8.1.

5.9 Ukončení TSP

Použijí se požadavky uvedené v ustanovení 7.12 normy ETSI EN 319 401 [3], které jsou definovány v samostatném dokumentu Politika pro KC a ČP, jakož i certifikační politika pro KC a ČP.

Dále platí tyto zvláštní pokyny:

a) Pokud jde o požadavek na odrážku b) iii) kapitoly 7.12 dokumentu Politika pro KC, jakož i certifikační politika pro KC a ČP., toto platí pro informace o registraci (viz články 6.2.2, 6.3.1 a 6.3.4), informace o stavu odvolání (viz článek 6.3.10) a události archivovat protokoly (viz články 6.4.5 a 6.4.6) na příslušné časové období, jak je určeno účastníkovi a spoléhající se straně (viz článek 6.8.10).



b) Pokud jde o požadavek d) článku 7.12 dokumentu Politika pro KC a certifikační politika pro KC a ČP. jsou zahrnuta i řešení stavu odvolání vydaných certifikátů, kterým neskončila platnost.

6 Technická bezpečnostní opatření

6.1 Generování a instalace párů klíčů

6.1.1 Generování páru klíčů certifikační autority

Klíče používané pro vydávání kvalifikovaných certifikátů a podepisování CRL a OCSP jsou generovány na HSM certifikovaném v souladu s nařízením eIDAS a příslušnými technickými normami.

Proces generování klíčů probíhá pod dvojí kontrolou zaměstnanců v důvěryhodných rolích za účasti třetí nezávislé osoby, která na něj dohlíží a formálně zaznamenává průběh. Jednotlivé role a odpovědnosti jsou popsány v dokumentaci Poskytovatele.

Privátní klíč se vygeneruje přímo na HSM a v žádném okamžiku jej neopouští v otevřené formě.

6.1.2 Generování klíčového páru Držitele

Má-li mít kvalifikovaný certifikát atribut, že klíč je umístěn na zařízení QSCD, musí být vygenerován na zařízení QSCD certifikovaném pro tento účel v souladu s nařízením eIDAS a příslušnými technickými normami, bez ohledu na to, zda je generován Poskytovatelem, jeho Registrační autoritou nebo přímo Držitelem. Poskytovatel sleduje platnost certifikace používaných zařízení.

Poskytovatel ani registrační autorita neuchovávají žádnou kopii soukromého klíče Držitele, s výjimkou případů, kdy je klíč Držitele generován přímo na zařízení Poskytovatele pro účely vzdáleného podepisování. Poskytovatel v tomto případě používá technické postupy a prostředky, které zaručují vysokou míru výhradní kontroly Držitele nad klíčem v souladu s příslušnými technickými normami [12].

6.1.3 Doručení soukromého klíče Držiteli

Soukromé klíče vygenerované Poskytovatelem nebo Registračním orgánem na kvalifikovaném prostředku pro vytváření podpisů/pečetí, které Poskytovatel neprovozuje, a autentizační údaje do zařízení budou předány Držiteli společně se zařízením osobně nebo důvěryhodným kanálem, který zajistí důvěrnost a integritu.

V případě klíčů generovaných na zařízení Poskytovatele je použití soukromých klíčů aktivováno Držitelem na dálku na základě autentizačních faktorů systému vzdáleného podepisování. Aktivační mechanismy jsou definovány v interním dokumentu.[1]

[1] Popis řešení vzdáleného QSCD v. 2.0, Ardaco, a.s.

6.1.4 Doručení veřejného klíče vystaviteli certifikátu

Veřejný klíč Držitele musí být doručen vydavateli certifikátu (Poskytovateli) ve formátu PKCS#10 Certification Request Format. Žádost musí být podepsána soukromým klíčem patřícím k veřejnému klíči. Žádosti musí předcházet identifikace a autentifikace podle kap. 3 na jejímž základě Poskytovatel jednoznačně asociuje PKCS#10 žádost s ověřenou identitou.

6.1.5 Předání veřejného klíče spoléhající se stranám

Veřejné klíče CA poskytovatele jsou zveřejňovány prostřednictvím evropského a národního seznamu důvěryhodných poskytovatelů služeb (TSL) a na webových stránkách poskytovatele. 0 a 1.6.3.

Veřejné klíče Držitelů Poskytovatelem není zveřejňováno, s výjimkou zveřejnění certifikátů s jejich výslovným souhlasem ve veřejném úložišti podle kapitoly. 1.6.3.

6.1.6 Délka klíče

Pro všechny typy certifikátů a algoritmů musí být nastavena minimální délka klíče. Délku klíčů určuje PMA v souladu s příslušnými technickými normami (ETSI TS 119 312), doporučeními Oránu dozoru a na základě bezpečnostních prvků konkrétních kryptografických zařízení.

6.1.7 Parametry a kvalita veřejného klíče

Parametry a kvalitu veřejných klíčů určuje PMA v souladu s příslušnými technickými normami (ETSI TS 119 312), doporučeními dozorového úřadu a na základě bezpečnostních prvků konkrétních kryptografických prostředků.

Stůl 1: Minimální délky klíče (bit):

Předmět	RSA	ECDSA
Poskytovatel	4096	-
Koncové entity	2048	256

6.2 Ochrana soukromého klíče a technická opatření pro kryptografický modul

6.2.1 Standardy pro kryptografické moduly

Poskytovatel na ochranu privátního klíče CA musí používat hardwarové moduly (HSM) certifikované podle eIDAS Protection Profile (PP) EN 419 221-5 " Cryptographic Module for Trust Services ". HSM musí být aktivován minimálně dvěma osobami v důvěryhodných rolích (duální kontrola). Privátní klíče nelze za žádných okolností exportovat z HSM v otevřené podobě.

HSM jsou chráněny před neoprávněnými změnami (tamper protection) a je s nimi bezpečně manipulováno v průběhu dodávky, uskladnění a používání. Při spuštění HSM jsou automaticky provedeny self-testy pro kontrolu správné funkčnosti HW a SW komponent.

6.2.2 Opatření na ochranu soukromého klíče (K nebo N)

Při jakékoli manipulaci se soukromými klíči CA je vyžadována přítomnost více osob. Žádný jednotlivec nedisponuje kompletními aktivačními údaji, které jsou potřebné pro přístup k libovolnému soukromému klíči CA.

6.2.3 Úschova klíčů Držitele (key escrow)

Poskytovatel neposkytuje úschovu klíčů Držitelů jako samostatnou službu. Klíče generované na zařízení Poskytovatele pro účely vzdáleného podepisování jsou aktivovány výhradně pomocí SAM, který je pro tento účel certifikován.

6.2.4 Zálohování soukromých klíčů

Klíče certifikační autority se generují a ukládají na zařízení, které splňuje požadavky podle 6.2.1 a který neumožňuje export klíče v otevřené podobě. Během zálohování je klíč exportován v zašifrované podobě tak, aby bylo dosaženo stejné nebo vyšší úrovně zabezpečení než původní klíč. Obnovení je technicky možné pouze při dodržení minimální dvojitý kontroly.

Klíče Držitele, které jsou spravovány Poskytovatelem pro vzdálené podepisování, jsou generovány na stejném typu zařízení se stejnými zálohovacími mechanismy, jak je popsáno výše.

Klíče držitele, které nejsou spravovány Poskytovatelem, nejsou Poskytovatelem zálohovány, a to ani v případě, že nejsou generovány na zařízení QSCD (tj. jsou generovány bez odpovídajícího atributu).

6.2.5 Archivace soukromých klíčů

Pro účely archivace se použije postup stanovený v 6.2.4. Archivované klíče jsou zničeny na konci doby uchovávání procedurou vyžadující dvojí řízení a nikdy nejsou obnoveny v produkčním provozu.

6.2.6 Zadávání privátních klíčů do kryptografického modulu

Klíče jsou generovány a ukládány na zařízeních, která splňují požadavky 6.2.1. Při obnovování soukromých klíčů ze zálohy je vyžadována duální kontrola.

6.2.7 Metody aktivace privátního klíče

Privátní klíče CA Poskytovatele lze aktivovat pouze za podmínek Poskytovatele. 6.2.2 (dvojí řízení). Aktivace probíhá pomocí čipové karty a přístupového hesla. Klíč je aktivován, dokud není deaktivován.

Soukromé klíče Držitele, které jsou spravovány Poskytovatelem, jsou aktivovány prostřednictvím SAM kapitoly. 6.2.3. Aktivace probíhá pomocí přihlašovacího hesla/ověřovacího kódu Držitele. Aktivace je platná vždy jen pro jednu operaci podepisování.

Aktivace soukromých klíčů Držitele, které nejsou v administraci Poskytovatele, je výhradní odpovědností Držitele.

6.3 Další aspekty správy párů klíčů

Klíče certifikační autority Poskytovatele sloužící k podepisování certifikátů a informace o jejich stavu nesmí být použity k žádnému jinému účelu a musí být použity výhradně ve fyzicky zabezpečených prostorách.

Použití klíčů certifikační autority musí být kompatibilní s algoritmy hash, podpisovými algoritmy a délkou klíče ve smyslu protokolu kap. 6.1.6 a 6.1.7.

Všechny privátní klíče certifikační autority musí být na konci svého životního cyklu zničeny.

6.4 Aktivační údaje

Aktivační údaje pro klíče certifikační autority poskytovatele musí být generovány v souladu s protokolem kap. 6.2.2.

Aktivační údaje pro klíče generované na zařízení určeném pro držitele musí být generovány způsobem, který zaručuje jejich důvěrnost, a musí být distribuovány zabezpečeným kanálem odděleným od zařízení (kap. 6.1.3)

6.5 Opatření pro zabezpečení počítače

Opatření pro bezpečnost počítačů se řídí bezpečnostní politikou schválenou vedením, která je přístupná a vhodně sdělená všem pracovníkům zajišťujícím provoz kvalifikovaných důvěryhodných službách. Přezkum a přezkum opatření v oblasti kybernetické bezpečnosti provádí Bezpečnostní rada.

6.6 Bezpečnostní opatření během životního cyklu

Použijí se požadavky uvedené v ustanovení 7.7 normy ETSI EN 319 401 [3], které jsou definovány v samostatném dokumentu Politika pro KC a certifikační politika pro KC a ČP.

6.7 Opatření pro zabezpečení sítě

Použijí se požadavky uvedené v ustanovení 7.8 normy ETSI EN 319 401 [3], které jsou definovány v samostatném dokumentu Politika pro KC a certifikační politika pro KC a ČP.

Dále se použijí tato zvláštní ustanovení:

a) organizace udržuje a chrání všechny systémy CA alespoň v zabezpečené zóně a implementuje a konfiguruje bezpečnostní postup, který chrání systémy a komunikaci mezi systémy v zabezpečených zónách a zónách s vysokým zabezpečením.
b) Organizace nakonfigurovala všechny systémy CA odebráním nebo zakázáním všech účtů, aplikací, služeb, protokolů a portů, které se nepoužívají při operacích certifikační autority.
c) Organizace uděluje přístup k zabezpečeným zónám s vysokým zabezpečením pouze důvěryhodným rolím.
d) Systém certifikační autority je v zóně s vysokým zabezpečením.

6.8 Použití časového razítka

Použijí se požadavky stanovené v ustanovení normy ETSI EN 319 421 [4], které jsou definovány v samostatném dokumentu Politika pro KC i certifikační politika pro KC a ČP.

7 Profily certifikátů, seznamy CRL a OCSP

Pravidla týkající se obsahu kvalifikovaného certifikátu pro elektronické podpisy:

a) označení ve formě vhodné pro automatizované zpracování, že certifikát se vydává jako kvalifikovaný certifikát pro elektronický podpis;
b) soubor údajů jednoznačně reprezentujících kvalifikovaného poskytovatele důvěryhodných služeb, který vydává kvalifikované certifikáty, zahrnující členský stát, ve kterém je tento poskytovatel usazen,
    a. v případě právnické osoby: název a případné registrační číslo, jak je uvedeno v úředních záznamech,
    b. v případě fyzické osoby: jméno osoby;
c) jméno podepisovatele nebo pseudonym s jasnou specifikací, že se jedná o pseudonym;
d) údaje pro validaci elektronického podpisu, které odpovídají údajům pro vyhotovení elektronického podpisu;
e) údaje o začátku a konci období platnosti osvědčení;
f) identifikační kód osvědčení, který je jedinečný pro kvalifikovaného poskytovatele důvěryhodných služeb;
g) zdokonalený elektronický podpis nebo zdokonalenou elektronickou Razítko vydávajícího kvalifikovaného poskytovatele důvěryhodných služeb;
h) lokalitu, na které je certifikát pro zdokonalený elektronický podpis nebo zdokonalenou elektronickou Razítko podle písmene g dostupný bezplatně;
i) lokalitu služeb, které lze využít ke zjištění statutu platnosti kvalifikovaného certifikátu;
    a. pokud se údaje pro vyhotovení elektronického podpisu související s údaji pro validaci elektronického podpisu nacházejí v zařízení pro vyhotovení kvalifikovaného elektronického podpisu/pečetě, ve formě vhodné pro automatizované zpracování.

Certifikáty vydané Poskytovatelem musí být ve formátu X.509 verze 3 podle RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [9].

7.1 Profil vydávající certifikační autority

7.1.1 Údaje vydávající certifikačního autority

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo přidělené Poskytovatelem
signatureAlgorithm	**sha256withRSAEncryption**
issuer	Shodné se subject (self-signed certifikát).
validity	
notBefore	Začátek platnosti certifikátu (UTCTime)
notAfter	Vypršení platnosti certifikátu (UTCTime) Max. 30 let
subject	ID certifikační autority přidružené k veřejnému klíči. Jednotlivé položky jsou uvedeny v následujících kapitolách.
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	Veřejný klíč subjektu
extensions	Rozšíření. Viz Rozšíření certifikátů vydávající certifikační autority
signature	Razítko certifikační autority zprostředkovatele (podepsaná svým držitelem)

7.1.2 Rozlišovací název vydávající certifikační autority

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
commonName	Ano	Identifikace – název CA pro kvalifikované důvěryhodných službách.
organizationalName	Ano	Oficiální název právnické osoby Poskytovatele.
organizationIdentifier	Ne	Identifikátor organizace, jak je uveden v příslušném rejstříku. Viz také Schémat dohledu kvalifikovanými důvěryhodných služeb podle definice orgánu dohledu [3].
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	Psč

7.1.3 Rozšíření certifikátu vydávající certifikační autority

Prodloužení	Kritický	Hodnota
basicConstraints	Ano	cA: TRUE pathlen:0
keyUsage	Ano	keyCertSign crlSign
certificatePolicies	Ne	CP, podle kterého byl certifikát vydán (tato CP) Policy 1.3.158.35829036.0.0.0.0
crlDistributionPoints	Ne	Nepřítomný
subjectKeyIdentifier	Ne	Identifikátor veřejného klíče držitele tohoto certifikátu.
authorityKeyIdentifier	Ne	Identifikátor veřejného klíče certifikačního úřadu, který tento certifikát vystavil.

7.2 Profil seznamu CRL

Seznamy CRL vydané Poskytovatelem musí být ve formátu X.509 verze 3 podle RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [9].

Pole	Hodnota
version	Hodnota (0x1)
signatureAlgorithm	sha256withRSAEncryption
issuer	Vydavatel seznamu CRL (CA)
thisUpdate	Datum a čas vydání CRL (UTC)
nextUpdate	Odhadované datum a čas vydání seznamu CRL (UTC)
revokedCertificates	Seznam zneplatněných certifikátů
userCertificate	pořadové číslo zneplatněného certifikát,
revocationDate	Datum a čas zneplatnění (UTC)
crlEntryExtensions	Rozšíření seznamu CRL
CRLReason	Důvod zneplatnění. Nesmí to být certificateHold.

crlExtensions	Rozšíření CRL
authorityKeyIdentifier	Identifikátor veřejného klíče certifikační autority, která vydala toto CRL.
signature	Elektronický razítko vydavatele CRL.

7.3 Profil OCSP

Profily požadavků a odpovědí OCSP jsou v souladu s dokumenty RFC 6960 a RFC 5019. Informace o stavu platnosti nebo zrušení kvalifikovaných certifikátů v odpovědi OCSP musí obsahovat kladné prohlášení o existenci a správnosti údajů.

Struktura odpovědí:

Pole	Povinný	Hodnota
ResponseStatus	Ano	0 nebo návratový kód chyby
ResponseBytes		
ResponseType	Ano	id-pkix-ocsp-basic
BasicOCSPResponse		
tbsResponseData		
Version	Ano	1
responderID	Ano	Distinguished Name OCSP respondéra
producedAt	Ano	Čas, ve kterém OCSP reponder podepsal odpověď.
Responses		
certID	Ano	Pole CertID podle RFC 6560
certStatus	Ano	Stav certifikátu
revocationTime	Ne	Čas zneplatnění nebo expirace (jako součást RevokedInfo v případě CertStatus revoked)
revocationReason	Ne	Důvod zneplatnění (jako součást RevokedInfo v případě CertStatus revoked)
thisUpdate	Ano	Čas, kdy byl stav načten z databáze
Archive Cutoff	Ne	
Extended Revoked Definition	Ne	NULL Označuje, zda respondér podporuje rozšíření podle bodu 2.2 RFC 6960
nextUpdate	Ano	Čas, kdy bude nejpozději k dispozici další aktualizace stavu certifikátu.
singleExtensions	Ano	Rozšíření
certHash	Ano	hodnota hash certifikátu, jehož stav je v *položce* certStatus objektu *SingleResponse*, podrobné vysvětlení viz Schéma dohledu NBU 5.2.13(d)
Nonce	Ne	Nonce z požadavku, pokud je uveden.
signatureAlgorithm	sha256WithRSAEncryption	Algoritmus použitý k podepsání odpovědi
signature	Ano	Podpis odpovědi
certificate	Ano	Certifikát respondéru OCSP

7.4 Profil certifikátu pro potvrzení existence a platnosti certifikátu (OCSP)

7.4.1 Položky certifikátu respondéru OCSP

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo přidělené Poskytovatelem
signatureAlgorithm	sha256withRSAEncryption
issuer	Vystavitel certifikátu (CA)
validity	
notBefore	Začátek platnosti certifikátu (UTCTime)
notAfter	Vypršení platnosti certifikátu (UTCTime)
subject	Viz rozcestník.
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	Veřejný klíč subjektu
extensions	Viz Rozšíření certifikátu respondéru OCSP
signature	Razítko zprostředkovatele certifikační autority

7.4.2 Rozlišující název certifikátu respondéru OCSP

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
commonName	Ano	Identifikace respondéru OCSP.
organizationalName	Ano	Oficiální název právnické osoby Poskytovatele.
organizationIdentifier	Ne	Identifikátor organizace, jak je uveden v příslušném rejstříku. Viz Schéma dohledu kvalifikovaných důvěryhodných služeb podle definice orgánu dohledu [3].

7.4.3 Rozšíření certifikátu respondéru OCSP

Prodloužení	Kritický	Hodnota
basicConstraints	Ano	cA: FALSE
keyUsage	Ano	digitalSignature nonRepudiation
extendedKeyUsage	Ano	id-kp-OCSPSigning
certificatePolicies	Ne	Policy 1.3.158.35829036.0.0.0.0 CPS: https://www.qsign.sk/tsp/ardaco_cp_qtsp_qc.pdf
crlDistributionPoints	Ne	https://tsp.ardaco.com/status/crl
OCSP No Check (1.3.6.1.5.5.7.48.1.5)	Ne	
subjectKeyIdentifier	Ne	Generovaný
authorityKeyIdentifier	Ne	Identifikátor veřejného klíče certifikační autority, který tento certifikát vystavil.

7.5 Profil kvalifikovaného certifikátu

7.5.1 Položky kvalifikovaného certifikátu

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo přidělené Poskytovatelem
signatureAlgorithm	Alespoň sha256withRSAEncryption pro RSA nebo Alespoň ecdsa-with-SHA256 pro ECDSA
issuer	Vydavatel certifikátu (CA)
validity	
notBefore	Začátek platnosti certifikátu (UTCTime)
notAfter	Vypršení platnosti certifikátu (UTCTime)
subject	Identifikace entity, která je přidružena k veřejnému klíči. Položky kvalifikovaného certifikátu pro podpis a razítko jsou uvedeny v následujících kapitolách.
subjectPublicKeyInfo	
algorithm	rsaEncryption nebo id-ecPublicKey
subjectPublicKey	Veřejný klíč subjektu
extensions	

7.5.2 Rozšíření. Vidět Rozlišovací jméno kvalifikovaného certifikátu pro webová sídla

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód státu.
serialNumber	Ne	Odkaz na identitu právnické osoby ve formátu podle dokumentu Schéma dohledu kvalifikovaných důvěryhodných služeb definované orgánem dohledu [3].
commonName	Ne	Zastaralé.
organizationalName	Áno	Název právnické osoby, jak je uvedeno v příslušném rejstříku.
organizationIdentifier	Nie (viď ale poznámky k hodnote)	Identifikátor organizace, jak je uvedeno v příslušném registru. V případě PSD2 certifikátů povinné - informace organizaci ve formátu podle ETSI TS 119 495.

	organizationalUnitName	Ne	Název organizační jednotky
	stateOrProviceName	Ne	Územní celek
	localityName	Ne	Obec
	streetAdress	Ne	Adresa ulice
	postalCode	Ne	Poštovní směrovací číslo
	Rozšíření kvalifikovaného certifikátů		
signature	Razítko poskytovatele CA.		

7.5.3 Rozlišovací název kvalifikovaného certifikátu k podpisu

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
givenName	Ano	Jména osob kromě příjmení.
surname	Ano	Příjmení
pseudonym	Pokud se jedná o certifikát obsahující pseudonym	Pseudonym
serialNumber	Ne	Odkaz na totožnost fyzické osoby ve formátu dokumentu Systém dohledu nad kvalifikovanými službami vytvářejícími důvěru definovaný orgánem dohledu [3].
commonName	Ano	Jméno a příjmení nebo pseudonym. V případě pseudonymu musí obsahovat řetězec "PSEUDONYM"
organizationalName	Ne	Název organizace držitele, jak je uveden v příslušném rejstříku.
organizationIdentifier	Ne	Identifikátor organizace, jak je uveden v příslušném rejstříku. Viz Schéma dohledu kvalifikovaných důvěryhodných služeb podle definice orgánu dohledu [3].
organizationalUnitName	Ne	Název organizační jednotky
title	Ne	Pozice nebo funkce
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	Psč

7.5.4 Rozlišovací název kvalifikovaného mandátního certifikát k podpisu

Podle § 8 odst. 1 písm. b) bodu 1 zákona č. 272/2016 Sb. jsou identifikační údaje klienta dle § 2 zákona č. 272/2016 Sb. uvedeny tak, že každá položka obsahující identifikační údaje klienta v položce subjektu certifikátu musí začínat řetězcem "MANDANT", aby nedošlo k záměně obsahu klienta a správce.

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
givenName	Ano	Jména osob kromě příjmení.
Surname	Ano	Příjmení

pseudonym	Pokud se jedná o certifikát obsahující pseudonym	Pseudonym
serialNumber	Ano	Odkaz na totožnost fyzické osoby ve formátu dokumentu Schéma dohledu kvalifikovaných důvěryhodných služeb definována orgánem dohledu [3]. Dále identifikační údaje klienta počínaje řetězcem MANDANT Příklad: SERIALNUMBER = IDCSK-HE1234 SERIALNUMBER = NTRSK-3456 SERIALNUMBER = MANDANT NTRSK-78910 Poznámka: Z hlediska požadavků Schématu dohledu NBU v.1.4 jsou identifikační údaje orgánu veřejné moci nebo osoby, u které mandatář vykonává činnost podle zvláštního právního předpisu nebo funkci podle zvláštního předpisu podle § 2 zákona č. 272/2016 Sb., uvedeny alespoň v položkách organizationName OID (2.5.4.10) a serialNumber OID (2.5.4.5) nebo organizationIdentifier OID (2.5.4.97) subjektu certifikátu. Pro tento profil byla zvolena alternativa serialNumber, a je proto povinná, i když schéma dohledu umožňuje jiné řešení
commonName	Ano	Jméno a příjmení, dále pro usnadnění neautomatizované manipulace s mandátním certifikátem zadejte textový řetězec " OPRÁVNENIE ", poté oddělte číslo autorizace xyz mezerou a poté oddělte textový název oprávnění ze seznamu registrovaných typů oprávnění (oprávnění) mezerou. Příklad: Petr Novák OPRÁVNENIE 1042 Advokát
organizationalName	Ne pro údaje o důvěryhodném subjektu Ano, pro povinná data.	Název organizace držitele, jak je uveden v příslušném rejstříku. Název orgánu veřejné moci nebo osoby, u které mandatář vykonává činnost podle zvláštního právního předpisu nebo vykonává funkci podle zvláštního předpisu, jak je uvedeno v příslušném rejstříku. Příklad: O = JUDr. Peter Polák O = MANDANT Slovenská advokátní komora
organizationIdentifier	Ne	Identifikátor organizace, jak je uveden v příslušném rejstříku.
organizationalUnitName	Ne	Název organizační jednotky

title	Ne	Pozice nebo funkce
stateOrProviceName	Ne	Územní jednotka
localityName*	Ne	Vesnice
streetAdress*	Ne	Ulice
postalCode*	Ne	Psč

* Data primárního dokumentu.

7.5.5 Rozlišovací název kvalifikovaného certifikátu pro Razítko

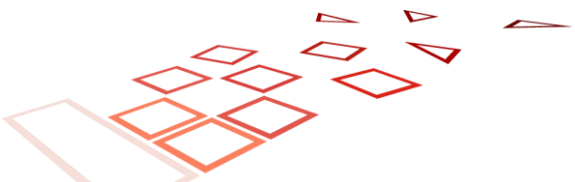
Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
serialNumber	Ne	Odkaz na totožnost právnické osoby ve formátu dokumentu Systém dohledu nad kvalifikovanými důvěryhodnými službami definovaný orgánem dohledu [3].
commonName	Ano	Popisný název právnické osoby nebo systému.
organizationalName	Ano	Název právnické osoby, jak je uveden v příslušném rejstříku.
organizationIdentifier	Ne	Identifikátor organizace, jak je uveden v příslušném rejstříku.
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	Psč

7.5.6 Rozlišovací jméno kvalifikovaného certifikátu pro webová sídla

Pole	Povinné	Hodnota
countryName	Áno	Dvojznakový kód státu.
serialNumber	Ne	Odkaz na identitu právnické osoby ve formátu podle dokumentu Schéma dohledu kvalifikovaných důvěryhodných služeb definované orgánem dohledu [3].
commonName	Ne	Zastaralé.
organizationalName	Áno	Název právnické osoby, jak je uvedeno v příslušném rejstříku.
organizationIdentifier	Nie (viď ale poznámky k hodnote)	Identifikátor organizace, jak je uvedeno v příslušném registru. V případě PSD2 certifikátů povinné - informace organizaci ve formátu podle ETSI TS 119 495.
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní celek
localityName	Ne	Obec
streetAdress	Ne	Adresa ulice
postalCode	Ne	Poštovní směrovací číslo

7.5.7 Rozšíření kvalifikovaného certifikátů

Prodloužení	Kritický	Hodnota
basicConstraints	Ne	cA: FALSE
keyUsage	Ano	digitalSignature



		nonRepudiation
extKeyUsage	Ne	emailProtection (1.3.6.1.5.5.7.3.4)
certificatePolicies	Ne	Certifikační politika NBU (1.3.158.36061701.0.0.0.1.2.2). Tato certifikační politika Jedna z politik QCP-n-qscd, QCP-l-qscd, QCP-l, QCP-n v závislosti na typu subjektu a na tom, zda je certifikát vydán kvalifikovanému prostředku pro vytváření elektronických podpisů/razítek. V případě mandátních certifikát navíc: 1.3.158.36061701.1.1.xyz – kde xyz je číslo oprávnění podle Seznamu oprávnění podle § 9 zákona č. 272/2016 Sb. Název (označení) autorizace by měl být uveden v jedné nebo více položkách typu UserNotice v položce explicitText jako utf8String o maximální velikosti 200 znaků alespoň ve slovenském jazyce
subjectAltName	Ne	Alternativní (nepovinné) jméno držitele certifikátu. Může zahrnovat například e-mail nebo jiné položky explicitně uvedené v RFC 5280 nebo lokálně definované položky (tj. vlastní OID), jako je identifikátor držitele používaný v rámci určité agendy v konkrétním systému.
subjectAltName	Ne (viď ale poznámky k Hodnota)	Alternativní (nepovinné) jméno Držitele certifikátu. Může zahrnovat např. e-mail případně jiné položky explicitně vyjmenované v RFC 5280, nebo lokálně definované položky (tj. custom OID) jako např. identifikátor Držitele, který používá v rámci určité agendy v konkrétním systému. V případě kvalifikovaných certifikátů pro autentifikaci webových sídel povinné - FQDN (Fully Qualified Domain Name).
crlDistributionPoints	Ne	Adresy pro získání informací o stavu certifikátů
qcStatement	Ne	id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD – pro certifikáty vydané kvalifikovanému prostředku pro vytváření elektronických podpisů a razítek id-etsi-psd2_qcStatement - pre PSD2 certifikáty
subjectKeyIdentifier	Ne	Identifikátor veřejného klíče držitele tohoto certifikátu.
authorityKeyIdentifier	Ne	Identifikátor veřejného klíče certifikačního úřadu, který tento certifikát vystavil.
nsComment	Ne	Volitelné doplňující informace k certifikátu (volný text).

8 Audit souladu a další hodnocení

Účelem auditu je potvrdit, že kvalifikovaný Poskytovatel důvěryhodných služeb a kvalifikované důvěryhodné služby, které poskytuje na základě této CP, splňují požadavky stanovené nařízením eIDAS. Poskytovatel musí podstoupit audit alespoň každých 24 měsíců nebo kdykoli na žádost orgánu dohledu v souladu s ustanoveními článku 20, bodů 1 a 2 nařízení eIDAS. Audit provádí akreditovaný subjekt posuzování shody v souladu s platnou legislativou pro důvěryhodné služby. Poskytovatel předloží výslednou zprávu o posouzení shody orgánu dohledu ve lhůtě tří pracovních dnů od jejího doručení.

Za odstranění případných nedostatků je zodpovědný bezpečnostní manažer. V případě nedostatků, které by zásadním způsobem znemožňovaly poskytování konkrétní služby, Poskytovatel přeruší její poskytování až do jejich odstranění.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

Poplatky za poskytnuté služby jsou uvedeny v aktuálním ceníku, který je uveden na internetových stránkách Poskytovatele dle kapitoly I. 0nebo se řídí jinou dohodou stran.

9.2 Finanční odpovědnost

Poskytovatel v souvislosti s rizikem odpovědnosti za škodu v souladu s článkem 13 nařízení eIDAS udržuje postačující finanční prostředky a/nebo uzavírá vhodné pojištění odpovědnosti za škodu v souladu s aplikovatelným právem.

Poskytovatel má uzavřeno a udržuje pojištění podnikatelských rizik v takovém rozsahu, aby byly pokryty případné finanční škody.

9.3 Důvěrnost obchodních informací

Důvěrnost obchodních informací se řídí platnými právními předpisy a smluvními vztahy mezi Poskytovatelem a jeho partnery a zákazníky.

9.4 Ochrana osobních údajů

Osobní údaje poskytnuté Poskytovateli jsou chráněny podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákona č. 18/2018 Sb. o ochraně osobních údajů.

Poskytovatel považuje za soukromé veškeré informace související s poskytováním důvěryhodných službách definované v dokumentu „Záznamy o spracovateľských činnostiach“, který je vytvořen na základě požadavku zákona č. 18/2018 Sb., o ochraně osobních údajů a o změně některých zákonů § 37 Evidence činností zpracování, s výjimkou:

a) aktuální informace, které mají být zveřejněny (např. ceníky, nabídky, kontaktní údaje)
b) Certifikační politika a prohlášení o certifikační politice
c) Certifikáty týkající se provozu důvěryhodných službách
d) Informace o stavu certifikátu
e) Infrastrukturní certifikáty
f) další informace, pokud s tím Objednatel výslovně souhlasí a Dodavatel má písemný souhlas Objednatele/Držitele

9.5 Práva duševního vlastnictví

Tato CP a všechny související dokumenty, jakož i obsah webových stránek, postupy Poskytovatele při poskytování důvěryhodných službách jsou chráněny autorským právem Poskytovatele.

9.6 Prohlášení a záruky

Jakékoli prohlášení, které má dopad na předplatitele i jiné relevantní strany nebo změny certifikační politiky a politiky bezpečnosti informací, jsou sdělovány předplatitelům i dalším příslušným stranám, hodnotícím orgánům, dozorným orgánům dohledu nebo jiným regulačním orgánům prostřednictvím veřejných internetových stránek společnosti.

9.7 Odmítnutí záruk

Poskytovatel odpovídá ve smyslu článku. 13 Nařízení eIDAS výhradně za škodu, kterou způsobí úmyslně nebo z nedbalosti jakékoli fyzické nebo právnické osobě tím, že nesplní své povinnosti podle tohoto Nařízení.
Poskytovatel neodpovídá za vady poskytnutých služeb v případě nesprávného nebo neoprávněného využívání služeb poskytnutých na základě Smlouvy o poskytování služeb držitelům certifikátu, zejména, nikoli však výlučně za využívání služeb v rozporu s podmínkami uvedenými v této CP.

Stížnosti a reklamace lze uplatnit emailem na adresy uvedené v bodě 1.3 této CP nebo doporučenou poštovní zásilkou na adresu sídla Poskytovatele. Stěžovatel/ reklamující (držitel certifikátu, zákazník nebo spoléhající se strana) je ve stížnosti/reklamaci povinna uvést minimální sériové číslo reklamovaného produktu a popis vady. Stížnost/ reklamace bude vyřízena Poskytovatelem ve lhůtě 30 dnů, pokud se strany nedohodnou jinak.

9.8 Omezení odpovědnosti

V případě delegovaných úkolů můžeme jako CA nebo jakákoli námi delegovaná třetí strana, smluvně si mezi sebou rozdělit odpovědnost, jak ji i určit, avšak jako CA budeme nadále plně zodpovědný za výkon všech stran v souladu s těmito požadavky, jako by úkoly nebyly delegovány. Odpovědnost externích subjektů je smluvně zajištěna a také zavazuje externí subjekty povinně provádět všechny kontroly námi vyžadované.

Také jako poskytovatel neodpovídáme za

- nepřímé či jiné ztráty nebo škody,
- za škodu (včetně ušlého zisku),

která vznikla zákazníkovi nebo držiteli certifikátu, spoléhající se straně příp. jakýmkoli třetím stranám z důvodu:

1. porušení povinností zákazníkem nebo držitelem certifikátu nebo spoléhající se stranou uvedených v právních předpisech, smlouvě, v politikách Poskytovatele, včetně povinnosti vynaložit přiměřenou péči při používání certifikátů a při spoléhání se na ně;
2. neposkytnutí potřebné součinnosti ze strany zákazníka a držitele certifikátu;
3. technickými vlastnostmi, konfigurací, nekompatibilitou, nevhodností nebo jinými vadami jimi použitých softwarových nebo hardwarových prostředků;
4. používání, resp. spoléhání se na certifikát, jehož platnost uplynula nebo který byl zrušen;
5. použití certifikátu Zákazníkem/Držitelem certifikátu v rozporu se smlouvou, politikami Poskytovatele;
6. použití certifikátu v rozporu s jeho určením nebo omezeními uvedenými v certifikátu, v politikách Poskytovatele;
7. prodlení nebo nedoručení požadavků na ověření statusu certifikátu Poskytovateli, z důvodů, které nejsou na straně Poskytovatele (zejména případy nedostupnosti nebo přetíženosti sítě internetu nebo chybami zařízení

nebo technického vybavení používaného ověřovatelem) nebo z důvodu nedostupnosti v průběhu plánované údržby nebo jiné organizační oznámené činnosti

8. působení vyšší moci.

Poskytovatel neodpovídá za škody, které vznikly spoléhající se straně z důvodu, že při spoléhání se na certifikát a důvěryhodné služby Poskytovatele, resp. na elektronický podpis nebo pečeť vyhotovené na jejich základě nepostupovala ve smyslu CP či CPS.

9.9 Kompenzace

Poskytovatel nenese odpovědnost za škody způsobené Zákazníkovi, držiteli nebo spoléhajícím se stranám v případě, že škoda byla způsobena v důsledku a/nebo v souvislosti s neplněním povinností vyžadovaných právními předpisy pro důvěryhodných službách, a to CPS i CP.

Poskytovatel neodpovídá za porušení svých povinností, pokud porušení těchto povinností bylo způsobeno vyšší mocí. Za vyšší moc se považuje zejména válka, požár, povodeň, velké přírodní anomálie, přerušení provozu, embargo, vládní opatření, pandemie, výbuch, jakož i výsledek jiných příčin mimo kontrolu poskytovatele. Tyto okolnosti jsou důvodem pro odklad plnění závazků ze strany Poskytovatele na dobu a v rozsahu, v jakém jsou tyto okolnosti účinné.

9.10 Podmínky a ukončení

Táto CP se vztahuje na všechny certifikáty vydané v souladu s ním až do skončení jejich platnosti.

S ohledem na ukončení jejich služeb se použije tento postup:

1) informovat o ukončení všechny účastníky a jiné subjekty, s nimiž máme dohody nebo jinou formu navázaných vztahů, mezi nimiž jsou spoléhající se strany, TSP a příslušné orgány, například orgány dohledu. Kromě toho budou tyto informace zpřístupněny dalším spoléhajícím se stranám;
2) ukončit všechna oprávnění všech subdodavatelů, které mohou jednat našem jménem při výkonu jakýchkoli funkcí týkajících se procesu vydávání tokenů důvěryhodných služeb.

9.11 Individuální oznámení a komunikace s účastníky

Oznámení a komunikace s Poskytovatelem probíhá prostřednictvím kontaktních údajů uvedených v kapitole 0. Poskytovatel může s účastníky komunikovat i jinými formami, a to na základě kontaktních údajů, které Poskytovateli poskytne. Proces řízení změn je jednotně definován v interním procesu řízení a schvalování změn.

9.12 Novelizace

Postup novelizace této CP je prováděn interně kontrolovaným procesem podle interní dokumentace. V případě jakýchkoliv změn se vždy změní verze dokumentu. V případě významných změn ve způsobu poskytování Služby musí být OID CP změněn. Jako kvalifikovaný poskytovatel důvěryhodných službách poskytujeme Národnímu bezpečnostnímu úřadu informace o změnách v jeho kvalifikovaných důvěryhodných službách nejpozději 30 dnů před plánovanou změnou podle jím stanovených postupů a pravidel. Informace o změnách se zveřejňují způsobem stanoveným v kapitole. 9.11.

9.13 Řešení sporů

Veškeré spory vzniklé v souvislosti s poskytováním důvěryhodných službách ze strany Poskytovatele budou řešeny především smírčím řízením mezi stranami sporu. Nebude-li dosaženo dohody o sporných nárocích do 30 pracovních dnů ode dne uplatnění nároku s druhou smluvní stranou, je kterákoli ze stran oprávněna podat žalobu k příslušnému soudu Slovenské republiky. Soudy Slovenské republiky jsou vždy příslušné k projednávání sporů se zahraničním prvkem.

9.14 Rozhodné právo

Vztahy mezi Poskytovatelem a Zákazníkem/Držitelem, jakož i činnost společnosti Ardaco a.s. se řídí právním řádem Slovenské republiky.

9.15 Soulad s platnými právními předpisy

Poskytovatel poskytuje důvěryhodné služby s platnou legislativou EU a SR, jakož i příslušnými mezinárodními standardy.
Je také zajištěna shoda se společnými kritérii EAL4+ pro HSM

9.16 Různá ustanovení

Poskytované důvěryhodných službách a produkty koncových uživatelů používané při poskytování těchto služeb musí být, pokud možno, přístupné osobám se zdravotním postižením.