ARDACO
DATA & COMMUNICATION SECURITY

Pravidla pro výkon certifikačních činností (CPS) Ardaco

Verze 1.5.13

Historie změn

Verze	Datum vydání	Schválený	Poznámka
1.0	19.2.2021	Richard Margala	První verze dokumentu.
1.1	14.5.2021	Richard Margala	Profil certifikátu zmocnění
1.2	28.7.2021	Richard Margala	Úprava textů kvalifikovaných certifikátů, jejichž soukromé klíče nejsou generovány v QSCD.
1.3	28.7.2021	Richard Margala	Doplnění Bezpečnostní rady jako odpovědné osoby, popis odstavce, § 6 odst. 2 zákona č. 272/2016 Sb., možnost použití elektronického podpisu Stanovená doba archivace záznamů. Přidány možnosti podepisování smluvní dokumentace. Přidáno sledování platnosti certifikace zařízení.
1.4.	28.7.2021	Richard Margala	Přidán profil časového razítka Přidán profil vystavující certifikační autority a respondéru OCSP a aktualizovány profily certifikátů. Byla aktualizována hierarchie certifikační autority.
1.5	1.9.2021	Richard Margala	Začlenění nedostatků do zprávy o posouzení shody společnosti Ardaco
1.5.1	16.12.2021	Richard Margala	Oprava terminologických chyb (kapitola 6.1 Zkratky)
1.5.2	3.3.2022	Richard Margala	Přidání aplikace také k následujícím službám • Kvalifikovaná důvěryhodná služba validace kvalifikovaných elektronických podpisů • Kvalifikovaná důvěryhodná služba validace kvalifikovaných elektronických pečetí
1.5.3	12.4.2023	Richard Margala	Doplnění požadavků na RA
1.5.4	30.5.2023	Richard Margala	Začlenění připomínek k auditu a změna okresního soudu Upřesnění profil certifikátu (nsComment).
1.5.4 aktualizace překladu 1	16.8.2023	Richard Margala	Formální úprava beze změny obsahu - korekce způsobu číslování zákonů v kap. 3.6.2
1.5.5	8.12.2023	Richard Margala	Doplnění seznamu zpřesňujících znaků pro uvádění dokladů v položce serialNumber.
1.5.6	8.12.2023	Richard Margala	Změna pojmu „Okresní soud Bratislava III“ na „Městský soud Bratislava III“
1.5.7	26.1.2024	Richard Margala	Opraveno formátování odstavce v 3.6.2 Ověření totožnosti fyzické osoby
1.5.8	31.1.2024	Richard Margala	Doplněna upřesnění k ověření oprávnění jednat kap. 3.6.3. Doplněna upřesnění k testovacím certifikátům v kap. 9.17. Doplněný postup při kompromitaci algoritmů v kap. 5.10.4 Doplněný postup při předávání citlivých údajů v kap. 5.3.2 Upřesněné lhůty pro výměnu CA klíče v kap. 5.9 Výměna klíčů Zapracování požadavku CSS-6.3.10-9A kap 4.10
1.5.9	9.5.2025	Richard Margala	Doplnění postup při překročení deklarované doby na zneplatnění certifikátu kap. 4.9.4. Upřesněné podmínky za kterých může být certifikát vydán po prvotním ověření identity v kap. 3.6.2 Upřesnění ke konzistenci CRL a OCSL v kap. 4.10 Odstraněna zmínka o povinnosti předávat vydané certifikáty a CRL NBÚ SR (novelizace právního předpisu).
1.5.10	12.6.2025	Richard Margala	Rozšíření podpory pro ověřování webových stránek.
1.5.11	1.11.2025	Richard Margala	Přidání požadavků podle standardů 319, 401 a NIS2
1.5.12	2.2.2026	Richard Margala	Začlenění pozorování z posledního auditu
1.5.13	30.3.2026	Richard Margala	Začlenění pozorování z posledního auditu Formální doplnění kapitoly 1.1 o 2 certifikované služby

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

1 ÚVOD 5

1.1 PŘEHLED 5
1.2 NÁZEV DOKUMENTU A JEDINEČNÁ IDENTIFIKACE 6
1.3 KONTAKTNÍ ÚDAJE 6
1.4 ZKRATKY 6
1.5 ÚČASTNÍCI INFRASTRUKTURY VEŘEJNÝCH KLÍČŮ 6
1.6 POUŽITÍ CERTIFIKÁTŮ 8

2 ZVEŘEJŇOVÁNÍ INFORMACÍ A ARCHIVŮ 9

3 IDENTIFIKACE A AUTENTIZACE 9

3.1 TYPY JMEN 9
3.2 SMYSLUPLNOST JMEN 10
3.3 ANONYMITA A POUŽÍVÁNÍ PSEUDONYMŮ 10
3.4 JEDINEČNOST JMEN 10
3.5 UZNÁVÁNÍ, OVĚŘOVÁNÍ A VÝZNAM OCHRANNÝCH ZNAČEK 10
3.6 POČÁTEČNÍ OVĚŘENÍ TOTOŽNOSTI 10
3.7 IDENTIFIKACE A AUTENTIZACE U ŽÁDOSTÍ O OPĚTOVNÉ VYDÁNÍ KLÍČE 13
3.8 IDENTIFIKACE A AUTENTIZACE PRO ŽÁDOSTI O ZRUŠENÍ PLATNOSTI CERTIFIKÁTU 14

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU 14

4.1 ŽÁDOST O CERTIFIKÁT 14
4.2 ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT 15
4.3 VYDÁNÍ CERTIFIKÁT 15
4.4 PŘEVZETÍ CERTIFIKÁTU 16
4.5 POUŽITÍ KLÍČOVÉHO PÁRU KLÍČŮ A CERTIFIKÁTU 16
4.6 OBNOVENÍ CERTIFIKÁTU 16
4.7 VYDÁNÍ NAVAZUJÍCÍHO CERTIFIKÁT 17
4.8 ZMĚNA CERTIFIKÁTU 17
4.9 ZRUŠENÍ A POZASTAVENÍ PLATNOSTI CERTIFIKÁTU 17
4.10 SLUŽBY OVĚŘOVÁNÍ STAVU CERTIFIKÁTŮ 19
4.11 UKONČENÍ POSKYTOVÁNÍ SLUŽEB 19
4.12 ÚSCHOVA A OBNOVA KLÍČŮ 20

5 FYZICKÁ BEZPEČNOST, ŘÍZENÍ A PROVOZNÍ OPATŘENÍ 21

5.1 OBECNÉ 21
5.2 BEZPEČNOSTNÍ POLITIKA (INFORMATION SECURITY POLICY) 21
5.3 SPRÁVA MAJETKU (ASSET MANAGEMENT) 22
5.4 FYZICKÁ BEZPEČNOSTNÍ OPATŘENÍ 22
5.5 PROCESNÍ OPATŘENÍ 23
5.6 PERSONÁLNÍ OPATŘENÍ 24
5.7 AUDITNÍ STOPY 25
5.8 UCHOVÁVÁNÍ ZÁZNAMŮ 26
5.9 VÝMĚNA KLÍČŮ 27
5.10 ZOTAVENÍ PO KOMPROMITACE A HAVÁRII 27
5.11 UKONČENÍ TSP 28

6 TECHNICKÁ BEZPEČNOSTNÍ OPATŘENÍ 29

6.1 GENEROVÁNÍ A INSTALACE PÁRŮ KLÍČŮ 29
6.2 OCHRANA SOUKROMÉHO KLÍČE A TECHNICKÁ OPATŘENÍ PRO KRYPTOGRAFICKÝ MODUL 30

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

6.3 Další aspekty správy párů klíčů 31
6.4 Aktivační údaje 32
6.5 Opatření pro zabezpečení počítače 32
6.6 Bezpečnostní opatření během životního cyklu 32
6.7 Opatření pro zabezpečení sítě 32
6.8 Použití časového razítka 32

7 PROFILY CERTIFIKÁTŮ, SEZNAMY CRL A OCSP 33

7.1 Profil vydávající certifikační autority 33
7.2 Profil certifikátu TSA 34
7.3 Profil certifikátu pro potvrzení existence a platnosti certifikátu (OCSP) 35
7.4 Profil kvalifikovaného certifikátu 36
7.5 Profil seznamu CRL 41
7.6 Profil OCSP 41
7.7 Profil časového razítka 42

8 AUDIT SOULADU A DALŠÍ HODNOCENÍ 43

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI 43

9.1 Poplatky 43
9.2 Finanční odpovědnost 44
9.3 Důvěrnost obchodních informací 44
9.4 Ochrana osobních údajů 44
9.5 Práva duševního vlastnictví 44
9.6 Prohlášení a záruky 44
9.7 Odmítnutí záruk 45
9.8 Omezení odpovědnosti 45
9.9 Kompenzace 45
9.10 Podmínky a ukončení 46
9.11 Individuální oznámení a komunikace s účastníky 46
9.12 Novelizace 46
9.13 Řešení sporů 46
9.14 Rozhodné právo 47
9.15 Soulad s platnými právními předpisy 47
9.16 Různá ustanovení 47

10 ODKAZY 48

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

1 Úvod

Tento dokument definuje pravidla pro výkon certifikačních činností společnosti Ardaco, a.s., se sídlem. Polianky 5, 841 01 Bratislava, zapsané v obchodním rejstříku Městského soudu Bratislava III, oddíl Sa, vložka č. 2903/B (dále jen "Ardaco" nebo "poskytovatel")

Základní rámec pro poskytování kvalifikovaných důvěryhodných služeb vytvářejících tvoří:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a důvěryhodných služeb 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 důvěryhodných službách pro elektronické obchody na vnitřním trhu a o změně některých zákonů (zákon o důvěryhodných službách)
- Systém dohledu nad kvalifikovanými službami vytvářejícími důvěru definovaný orgánem dohledu – NBÚ SR
- Zákon č 69 z 30. leden 2018 o kybernetickej bezpečnosti a o změne a doplnení niektorých zákonov
- SMĚRNICE (EU) 2022/2555 EVROPSKÉHO PARLAMENTU A RADY ze dne 14. prosince 2022 týkající se opatření pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii, změny nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)
- Nařízení (EU) 2024/1183 Evropského parlamentu a Rady ze dne 11. dubna 2024, které mění nařízení (EU) č. 910/2014

1.1 Přehled

Pravidla pro výkon certifikačních činností (CPS) Ardaco (Certificate Practice Statement, dále jen "CPS") společnosti Ardaco, a.s. slouží jako podklad pro účastníky PKI k posouzení důvěryhodnosti certifikátu.

CPS podporuje certifikační autoritu pro následující služby:

- Kvalifikovaná důvěryhodná služba pro vytváření a ověřování kvalifikovaných certifikátů pro elektronický podpis
- Kvalifikovaná důvěryhodná služba pro vytváření a ověřování kvalifikovaných certifikátů pro elektronické razítko
- Kvalifikovaná důvěryhodná služba pro vytváření kvalifikovaných elektronických časových razítek
- Kvalifikovaná důvěryhodná služba pro ověřování kvalifikovaných elektronických podpisů
- Kvalifikovaná důvěryhodná služba pro ověření kvalifikovaných elektronických razítek
- Kvalifikovaná důvěryhodná služba pro vytváření a ověřování kvalifikovaných certifikátů pro ověřování webových stránek
- Kvalifikovaná důvěryhodná služba pro správu zařízení pro vzdálené vytváření kvalifikovaných elektronických podpisů
- Kvalifikovaná důvěryhodná služba pro správu zařízení pro vzdálené vytvoření kvalifikované elektronické pečeti

Plnění CP KCA NBÚ při vydávání a ověřování kvalifikovaných certifikátů je dle 5.2.1 SD Čl. Čl. 5, Čl. 24, 28, 38 a 45 nařízení (EU) č. 910/2014 postup plnění požadavků národní legislativy je uveden zejména v kapitole 10 v certifikační politice kořenové certifikační autority NBÚ (CP KCA NBÚ) OID (1.3.158.36061701.0.0.0.1.2.2), která profiluje ETSI EN 319. (2016-02) [8] certifikační politiky pro vydávání kvalifikovaných certifikátů.

Pro poskytování kvalifikované důvěryhodné služby pro vytváření kvalifikovaných elektronických časových razítek platí rovněž podmínky stanovené v dokumentu "Certifikační politika kvalifikované důvěryhodné služby pro vytváření kvalifikovaných elektronických časových razítek".

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

1.2 Název dokumentu a jedinečná identifikace

Název dokumentu (jedinečná identifikace)	Pravidla pro výkon certifikačních činností (CPS) Ardaco ver. 1.5.13
OID	Neuděleno

1.3 Kontaktní údaje

Adresa sídla společnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovensko
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail s hlášením incidentů:	incidents@ardaco.com

1.4 Zkratky

CA	Certifikační autorita
CP	Certifikační politika
CPS	Pravidla pro výkon certifikačních činností
CRL	Seznam odvolaných certifikátů (Certification Revocation List)
ČP	Časové razítko
KC	Kvalifikovaný certifikát
PKI	Infrastruktura veřejných klíčů (Public Key Infrastructure)
RA	Registrační autorita
QSCD	Zařízení pro vyhotovení kvalifikovaného elektronického podpisu (Qualified Signature Creation Device)
TSP	Poskytovatel Důvěryhodný služeb (Trusted Services Provider)

1.5 Účastníci infrastruktury veřejných klíčů

1.5.1 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).

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 záznamu důvěryhodných položek	TLISK-133

1.5.2 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 .

TSP má uzavřenou zdokumentovanou dohodu a smluvní vztah, pokud poskytování služeb zahrnuje subdodávky, outsourcing nebo jiná ujednání se třetí stranou, aby bylo zajištěno jasné porozumění mezi TSP a dodavatelem, pokud jde o povinnosti obou stran plnit příslušné požadavky na bezpečnost informací.

1.5.3 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.

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

(zaměstnanci, konatele apod.). Povinnosti Držitele a Zákazníka jsou uvedeny ve Smlouvě o vydávání a používání kvalifikovaného certifikátu.

1.5.4 Spoléhající se strany

Spoléhající se strany jsou subjekty, které se při své činnosti spoléhají na výstupy poskytování důvěryhodných služeb podle tohoto CPS.

1.5.5 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.

1.5.6 Ostatní účastníci

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

TSP zajišťuje uplatňování informační bezpečnosti v souladu se zavedenou politikou informační bezpečnosti, tematicky specifickými politikami a postupy TSP. Toto dodržování je zajištěno, buď smluvní dohodou nebo prokázáním relevantní certifikace jako je např. ISO27001 nebo ekvivalent bezpečnostní normy.

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.

1.6 Použití certifikátů

Kvalifikované certifikáty lze používat pouze v souladu s platnými právními předpisy. Kvalifikovaný certifikát podle tohoto CPS 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]

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

- 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]
- fyzická nebo právnická osoba za účelem ověřování webových stránek podle článku 3(38) a článku 45 nařízení eIDAS [QEVCP-w]

2 Zveřejňování informací a archivů

Certifikáty musí být umístěny tak, aby byly přístupné držitelům, zákazníkům a spoléhajícím stranám. Funkci úložiště certifikátů plní webové stránky Poskytovatele dle kapitoly 1.3. Webové stránky jsou veřejně dostupné. Přístup k informacím o certifikátech certifikačních autorit Poskytovatele je veřejně dostupný bez omezení. Poskytovatel nezveřejní konečné certifikáty Držitelů ve svém sídle bez získání přímého souhlasu Držitele nebo subjektu, pro který je certifikát vydán, s výhradou následujících pravidel.

a) Po vygenerování bude certifikát zpřístupněn držiteli nebo subjektu, pro který je certifikát vydán.
b) Certifikáty jsou k dispozici pro vyhledávání pouze v těch případech, pro které byl získán souhlas subjektu. Je-li subjektem zařízení nebo systém, musí být namísto subjektu získán souhlas fyzické nebo právnické osoby odpovědné za provoz zařízení nebo systému.
c) Poskytovatel zpřístupní spoléhajícím se stranám podmínky týkající se používání certifikátu (viz odstavec 6.9.4).
d) Příslušné podmínky musí být pro toto certifikát snadno identifikovatelné.

CP, CPS je schválena a upravena v souladu s definovaným procesem "GL-450-Kontrola dokumentů", včetně odpovědnosti za udržování CP, CPS a jejich aktualizací.

Veškeré změny CP, jakož i CPS nebo podmínek musí být a budou zveřejněny na webových stránkách (viz bod "Internetová adresa" v kapitole 1.3 Kontaktní údaje)

Oznamování důležitých změn v poskytování důvěryhodné služby příslušným stranám v souladu s obchodními požadavky a příslušnými zákony a předpisy, včetně změn v poskytování důvěryhodných služeb a záměru ukončit její poskytování bude publikováno na webovém sídle „Internetová adresa“ v kapitole 1.3 Kontaktní údaje. Rovněž bude postupováno na základě Plánu ukončení činností. Všechny relevantní i spoléhající se strany v předstihu budou informovány podle požadavků zákona.

3 Identifikace a autentizace

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]

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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.

3.6.2 Ověření identity fyzické osoby

Poskytovatel musí ověřit totožnost fyzické osoby a případné specifické atributy, které jsou uvedeny v certifikátu.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

Svou identitu můžete ověřit jedním z následujících způsobů:

a) ukazující primární a sekundární důkazy
b) podpisem klíčem, který náleží kvalifikovanému certifikátu, přičemž tento původní kvalifikovaný certifikát
    - byl vydán Poskytovatelem, čímž není dotčena povinnost Poskytovatele ověřit aktuálnost údajů, nebo
    - jde o kvalifikovaný certifikát vydaný na elektronický občanský průkaz s čipem dle § 4 Zákona č. 395/2019 Sb. o občanských průkazech a o změně a doplnění některých zákonů a Poskytovatel ověří živost osoby
c) prokázáním se primárním dokladem a záznamem o provedení kontroly aktuálnosti údajů vůči spolehlivému zdroji (např. Registr fyzických osob, Registr obyvatel) a to zejména v případě, že je registrační autoritou banka, přičemž byla osoba identifikována ve smyslu AML předpisů
    - v SR: zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov
    - v ČR: zákon č. 253/2008 Sb. zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorizmu
    - v jiných státech vnitrostátní předpis adresující problematiku AML za dodržení podmínky prokázání se primárním dokladem a kontroly aktuálnosti údajů

Primárním dokumentem je:

a) pro občany Slovenské republiky je občanský průkaz nebo cestovní pas
b) státní příslušníci jiných členských států EU: doklad totožnosti používaný k prokázání totožnosti na území daného členského státu nebo cestovní pas
c) pas pro ostatní cizince

Sekundárním dokladem je:

a) Občanský průkaz
b) cestovní pas
c) řidičský průkaz
d) zbrojní průkaz
e) Servisní karta

Za jednoznačně identifikovatelnou se považuje tato kombinace:

a) celé jméno a příjmení osoby (současné i při narození)
b) osobní identifikační číslo, je-li dané osobě přiděleno (jedná se o jedinečný identifikátor vytvořený vysílajícím členským státem v souladu s technickými specifikacemi pro účely)
c) datum narození, pokud osoba nemá přiděleno rodní číslo
d) adresa trvalého pobytu
e) číslo předkládaného dokladu (platí pro všechny předkládané doklady).

Ověření identity fyzické osoby lze provést i předložením dokladů v kombinaci –

- primární a primární doklad nebo
- primární a sekundární doklad, za předpokladu, že obsahuje požadované údaje potřebné pro jednoznačnou identifikaci.

Poskytovatel musí vytvořit záznam ověření identity, který obsahuje všechny následující položky:

a) jedinečné identifikační údaje ověřované osoby dle předchozího odstavce
b) identifikace případných prostředků použitých k identifikaci osoby;
    - doklad – jeho číslo, vydavatel a datum platnosti (je-li označen)
    - Kvalifikovaný certifikát – běžný název, sériové číslo a vydavatel
    - transakce – číslo transakce, číslo účtu odesílatele a příjemce
c) identifikace osoby, která provedla identifikaci
d) datum identifikace

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

Registrace čísla dokumentu probíhá dvěma způsoby:

1. ručním přepisem,
2. automatickým přepisem.

Za předpokladu, že před vydáním certifikátu je ověřena aktuálnost údajů žadatele, dodržena všechna další ustanovení veřejných a interních předpisů Poskytovatele a podmínky použití služby, Poskytovatel neomezuje časový interval mezi prvotním ověřením identity a následným (i opakovaným) vydáním certifikátu.

3.6.3 Ověření oprávnění jednat

Ověření oprávnění k jednání je nezbytné pro vydání mandátního certifikátu podle § 8 zákona č. 272/2016 Sb.

Při žádosti o mandátní certifikát musí žadatel prokázat oprávnění budoucího držitele:

a) jednat jménem nebo jménem klienta (fyzické nebo právnické osoby),
b) vykonává činnosti podle zvláštního právního předpisu, nebo
c) vykonávat funkci podle zvláštního předpisu.

Oprávnění se prokazuje podle seznamu dokumentů, které jsou u daného oprávnění uvedeny v seznamu oprávnění podle § 9 zákona č. 272/2016 Sb., o důvěryhodných službách pro elektronické obchody na vnitřním trhu a o změně některých zákonů.

Doklad použitý k ověření oprávnění k jednání musí být originál nebo úředně ověřená kopie.

Poskytovatel může rovněž akceptovat hromadný seznam oprávněných osob a jejich oprávnění k prokázání svého oprávnění. Seznam musí být autorizován statutárním orgánem organizace, která o vydání mandátního certifikátu žádá, nebo jinou oprávněnou osobou.

Hromadný seznam musí obsahovat:

a) jméno a příjmení osoby, které má být mandátní certifikát vydán,
b) Typ a číslo identifikačního dokladu
c) Číslo oprávnění

Poskytovatel musí vytvořit záznam ověření identity, který obsahuje všechny následující položky:

a) identifikaci prostředků použitých prokázání oprávnění jednat (číslo dokladu, pokud existuje, vydavatel, datum platnosti)
b) identifikace osoby, která provedla identifikaci
c) datum identifikace

V případě, že se nejedná o vydání mandátního certifikátu podle § 8 zákona č. 1/2003 272/2016 Z. z, ale je ověřován vztah k organizaci za účelem vydávání certifikátů v jiných členských státech EU, aplikují se postupy ověřování jako u mandátních certifikátů s výjimkou používání seznamu oprávnění jako autoritativního zdroje pro seznam požadovaných dokladů. V případě jakýchkoli pochybností o relevanci předloženého dokladu pro prokázání vztahu, nelze certifikát vydat.

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

K ověření totožnosti právnické osoby se používá výpis z rejstříku, ve kterém je právnická osoba zapsána (např. obchodní rejstřík, živnostenský rejstřík, rejstřík neziskových organizací apod.), v případě zahraniční osoby v rejstříku příslušného státu

Doklad použitý k ověření oprávnění k jednání musí být originál nebo úředně ověřená kopie. Doklad nesmí být starší 30 dnů. V případě, že tento doklad nelze spolehlivě ověřit, certifikát poskytovatel nesmí vydat.

Minimální soubor údajů pro právnické osoby

a) Minimální soubor údajů pro právnické osoby obsahuje všechny tyto povinné atributy:
    a. současný úřední název (názvy),
    b. jedinečný identifikátor vytvořený předávajícím členským státem v souladu s technickými specifikacemi pro účely přeshraniční identifikace a pokud možno následně nezměněný.
b) Minimální soubor údajů pro právnické osoby obsahuje jeden nebo více z těchto povinných atributů:
    a. současná adresa,
    b. Registrační číslo DPH,
    c. daňové registrační číslo,
    d. identifikátor (identifikační znak) podle čl. 3 odst. 1 směrnice Evropského parlamentu a Rady 2009/101/ES (1),
    e. identifikátor právnické osoby (LEI) uvedený v prováděcím nařízení Komise (EU) č. 1247/2012 (2),
    f. registrační a identifikační číslo hospodářského subjektu (EORI) uvedené ve vykonávacím nařízení Komise (EU) č. 1352/2013 (3);

Při vydávání kvalifikovaných certifikátů pro autentifikaci webových sídel se postup ověřování provádí v souladu s požadavky standardu CA/Browser Forum – Guidelines pro průvodce a management of Extended Validation Certificates.

V případě uvádění PSD2 atributů je Poskytovatel ověřuje vůči veřejnému registru podle PSD2 (rejstřík NBS ČR nebo jiné příslušné národní kompetentní autority ve smyslu PSD2).

Poskytovatel musí vytvořit záznam ověření identity, který obsahuje všechny následující položky:

a) identifikaci prostředků použitých prokázání oprávnění jednat (číslo dokladu – pokud existuje, vydavatel, datum platnosti)
b) identifikace osoby, která provedla identifikaci
c) datum identifikace

3.6.5 3.6.5 Ověření kontroly nad doménou

Ověření toho, že Zákazník je vlastníkem domény resp. má kontrolu nad danou doménou, jejíž FQDN se nachází v položce CN žádosti, resp. bude uvedeno v položce Subject Alternative Name (SAN), je provedeno následovně:

- Poskytovatel vyžádá umístění náhodně vygenerované hodnoty nebo žádacího tokenu v DNS záznamu typu CNAME, TXT nebo CAA buď pro autorizovanou doménu (Authorization Domain Name), nebo pro autorizovanou doménu s předponou doménové části (Domanin Label) začínající podtržítkem (_).
- Náhodná hodnota musí být jedinečná pro každou žádost o vydání certifikátu a nesmí být použita opakovaně.

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

certifikát platného v době podání žádosti. Poskytovatel může takové ověření identity řetězit prostřednictvím jím vydaného kvalifikovaného certifikátu nejdéle po dobu 10 let.

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 zrušení platnosti 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

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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

Registrační proces lze provést:

a) na místě, osobní návštěvou CA nebo RA
b) na dálku, s technickými prostředky poskytujícími stejnou úroveň záruk ověření totožnosti jako při osobní návštěvě

Žadatel zejména:

a) poskytnout pravdivé a úplné informace nezbytné pro vydání certifikát
b) připravit a předložit dokumenty potřebné pro ověření totožnosti a vydání certifikát
c) seznámit se a odsouhlasit Smlouvou o vydávání a užívání kvalifikovaného certifikátu a souhlasu se zpracováním osobních údajů
d) zvolit vhodné heslo pro odvolání certifikátu (min. požadavky jsou uvedeny v dokumentaci pro vystavení certifikátu)

Poskytovatel je zejména povinen:

a) musí věnovat náležitou pozornost výkonu všech činností souvisejících s poskytováním kvalifikovaných služeb
b) informovat Žadatele o podmínkách
c) ověřovat údaje obsažené v předložených dokumentech v přiměřeném rozsahu
d) pokud dvojice klíčů není generována Poskytovatelem, ověřit, zda subjekt vlastní nebo ovládá privátní klíč spojený s veřejným klíčem, který byl předložen k vydání certifikátu
e) pokud má certifikát obsahovat atribut, že klíč je umístěn na QSCD, ověřte tuto skutečnost

Žadatel může podepsat požadovanou dokumentaci:

1. zdokonaleným nebo kvalifikovaným podpisem pomocí specializovaných nástrojů.
2. zasláním podepsané dokumentace v listinné podobě.

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 VYKONÁVACÍM 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. 2003/2003 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu. Daný popis řešení je garantován certifikační politikou pro kvalifikovaný certifikát.

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.

V případě kvalifikovaných certifikátů pro autentifikaci webových sídel Poskytovatel musí získat a zpracovat záznamy CAA v souladu s RFC 8659 pro každé dNSName v rozšíření subjectAltName.

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).

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 2. Aplikují se omezení pro zveřejňování osobních údajů.

4.4.3 Oznámení o vydání certifikát jiným stranám

Neuplatňuje sa.

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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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:

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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. 1.3. 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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

4.9.4 Doba zpracování žádosti

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

Postup při překročení deklarované doby Poskytovatel má interní proces, který generuje automatická upozornění na nezpracované žádosti a interní eskalační procedury. V případech, kdy přesto dojde k překročení deklarované doby na zneplatnění, poskytovatel informuje žadatele o zpoždění. Oznámení bude obsahovat vysvětlení důvodu zpoždění, očekávaný čas na vyřešení problému a kontaktní údaje pro další otázky. Všechny incidenty překročení doby musí být důkladně zdokumentovány a řešeny v rámci interního procesu pro řešení incidentů.

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. 2). 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.

OCSP odpovědi vždy odrážejí aktuální stav v době požadavku. V případě, že certifikát byl zneplatněn po vydání posledního CRL, ale před generováním OCSP odpovědi, bude tento stav v OCSP dostupný dříve než v dalším CRL

Ověření platnosti certifikátu k času podpisu není možné vůči CRL, pokud je doba podpisu po době vydání posledního CRL, protože CRL nepokrývá stav po této době. V takovém případě je výsledek ověření považován za neúplný, dokud není dostupné novější CRL nebo OCSP odpověď. V případě rozdílů mezi CRL a OCSP má přednost OCSP jako aktuálnější zdroj.

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 zrušení certifikátu v CRL a OCSP jsou v průběhu času konzistentní, přičemž je třeba zohlednit různá zpoždění při aktualizaci informací o stavu pro obě metody. V případě OCSP jsou publikovány po zrušení, a v případě CRL nejpozději v nejbližší aktualizaci. V CRL nebo OCSP odpovědi jsou udržovány minimálně do doby expirace certifikátu.

4.11 Ukončení poskytování služeb

Podmínky ukončení poskytování služeb jsou uvedeny v obchodních podmínkách.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

4.12 Úschova a obnova klíčů

Poskytovatel tuto službu neposkytuje.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

5 Fyzická bezpečnost, řízení a provozní opatření

5.1 Obecné

Použijí se požadavky uvedené v ustanoveních 5, 6.3 a 7.3 normy ETSI EN 319 401 [3], které jsou definovány v samostatném dokumentu Politika Ardaco, jakož i certifikační politika pro KC a ČP. Rovněž se uplatňují požadavky uvedené v ustanovení 6.4.1 normy ETSI EN 319 411-2 [1], které jsou definovány v samostatném dokumentu Politika Ardaco i certifikační politika pro KC a ČP.

5.1.1 Hodnocení rizika

Poskytovatel provede posouzení rizika s cílem identifikovat, analyzovat a vyhodnotit rizika důvěryhodných služeb s přihlédnutím k obchodním a technickým problémům. Následně identifikuje a vybere vhodná opatření k ošetření rizika s přihlédnutím k výsledkům posouzení rizika. Opatření k ošetření rizika zajistí, aby úroveň bezpečnosti byla přiměřená stupni rizika.
Rizikový management je plně integrován v rámci stávajících procesů řízených podle normy ISO9001 s integrovanými vybranými a platnými postupy definovanými normou ISO27005.

5.1.1.1 Hodnocení rizika

Poskytovatel posoudí organizační rizika alespoň během přezkoumání vedením organizace a zároveň uchovává dokumentované informace. Další možností hodnocení rizik je pravidelně jak na projektových schůzkách, tak na schůzkách jednotlivých oddělení organizace. Následně jsou rizika průběžně řešena podle výskytu a majitele.

Rizika projektu jsou zaznamenána v dokumentu "Risk assessment". IT rizika (do této skupiny patří i bezpečnostní rizika) jsou evidována na procesním portálu za účelem poskytnutí řešení na úrovni managementu. Tyto dohodnuté kroky jsou následně zaznamenány do interního systému nebo vytvořením samostatného interního projektu.

Postup celého procesu je definován v samostatném dokumentu nazvaném " Risk Managment".

5.2 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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

Konfigurace systémů je také pravidelně kontrolována na změny, které porušují bezpečnostní politiky, minimálně jednou za 12 měsíců během roku.

5.3 Správa majetku (Asset management)

5.3.1 Obecné požadavky (General requirements)

Organizace zajišťuje přiměřenou úroveň ochrany svých aktiv včetně informačních aktiv. Také vede inventarizaci všech informačních aktiv a přiděluje klasifikaci v souladu s hodnocením rizika, jako samostatný dokument.

5.3.2 Manipulace s médii

Se všemi nosiči se zachází bezpečně v souladu s požadavky systému klasifikace informací. Nosiče obsahující citlivé údaje musí být bezpečně odstraněny, pokud již nejsou potřebné.

Proces správy médií je definován jako samostatný dokument.

V případě, že jsou předávány citlivé údaje, např.: PIN a PUK ke kartám, či jiná hesla v papírové formě, musí být takové informace předávány v zapečetěné obálce.

Organizace má smluvně definovaná pravidla sdílení informací týkajících se dodavatelského řetězce a jakýchkoli potenciálních problémů a kompromisů mezi TSP a jeho dodavateli.

5.4 Fyzická bezpečnostní opatření

5.4.1 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.

5.4.2 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.

5.4.3 Napájení a klimatizace

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

5.4.4 Ochrana před vodou

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

5.4.5 Ochrana před ohněm

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

5.4.6 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.

5.4.7 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.

5.5 Procesní opatření

5.5.1 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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

- **RA Operator:** zajišťuje registraci a ověření totožnosti Zákazníků a Držitelů a informací obsažených v certifikátu, schvaluje žádosti o vydání a zneplatnění certifikátu.

5.5.2 Počet osob vyžadován na výkon činností

Zabezpečeno v souladu s interními provozními postupy.

5.5.3 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.

5.5.4 Nekompatibilita rolí

Zabezpečeno v souladu s interními provozními postupy.

5.6 Personální opatření

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

5.6.1 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.

5.6.2 Postupy detekční kontroly

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

5.6.3 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.

5.6.4 Požadavky, rekvalifikace personálu a jejich četnost

Viz kap. 5.6.3

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

5.6.5 Frekvence a posloupnost otáčení válce

Řídí se vnitřními organizačními pravidly Poskytovatele.

5.6.6 Sankce za nepovolené činnosti

Řídí se vnitřními organizačními pravidly Poskytovatele podle stupně závažnosti přestupku.

5.6.7 Dokumentace, kterou musí poskytnout zaměstnanci

Pro výkon každé funkce je zaměstnancům prokazatelně poskytována dokumentace v nezbytném rozsahu (viz 5.6). Pracovníci jsou povinni používat dokumenty pouze k určenému účelu.

5.7 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.

5.7.1 Typy protokolovaných událostí

Zprostředkovatel protokoluje následující typy událostí.

- Životní cyklus držitelů certifikátů
  - Žádosti o vydání KC, včetně registračních údajů a výsledků jejich ověření
  - Záznamy o vydaní KC
  - Záznamy o převzatí KC
  - Žádosti o zrušení KC a výsledky jejich prověření
- Životní cyklus klíče CA
  - jakákoli manipulace s klíčovým párem CA (generování, zálohování a obnovení, zneplatnění)
- Zařízení pro vyhotovení kvalifikovaného elektronického podpisu/razítek
  - Záznamy o jejich přípravě
- Publikování
  - Evidence zrušených KC
  - Evidence tvorby a publikování seznamů zrušení KC
- Bezpečnost a infrastruktura
  - Záznamy o změnách zásad zabezpečení, spouštění a vypínání systému, pádech systému a selháních hardwaru, aktivitách brány firewall a směrovače a pokusech o synchronizaci času systému PKI.
  - Záznamy o instalacích, aktualizacích a změnách konfigurace
  - Evidence provozních a bezpečnostních incidentů a jejich řešení

5.7.2 Frekvence zpracování záznamů

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

5.7.3 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. 5.8.2.

5.7.4 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.

5.7.5 Postupy pro zálohování záznamů auditu

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

5.7.6 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.

5.7.7 Oznámení subjektu, který událost způsobil

Neuplatňuje se.

5.7.8 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 Ardaco a certifikační politika pro KC a ČP.

5.8 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.

5.8.1 Typy archivovaných záznamů

Poskytovatel archivuje záznamy minimálně v následujícím rozsahu:

- záznamy podle 5.7.1
- vydány certifikáty
- seznamy zrušených certifikátů
- oficiální korespondence
- bezpečnostní dokumentace
- instalační média

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

5.8.2 Doba uchovávání

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

5.8.3 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.

5.8.4 Postupy zálohování

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

5.8.5 Požadavky na přidávání časových razítek

Neuplatňuje se.

5.8.6 Systém sběru archivů

Neuplatňuje se.

5.8.7 Postupy pro získávání a ověřování archivních informací

Neuplatňuje se.

5.9 Výměna klíčů

Výměna klíčů se provádí:

- před vypršením platnosti certifikátu CA - minimálně 30 dní předem, optimálně však s takovým předstihem, aby výměna CA klíčů neovlivňovala délku platnosti vydávaných koncových certifikátů
- v případě ohrožení zabezpečení nebo důvodného podezření na ohrožení soukromého klíče certifikační autority

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

5.10 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.

5.10.1 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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

hodin nebo v souladu s platnými zákony. V rámci postupu je také určena jedna osoba odpovědná za bezpečnost sítě a informací a podávání zpráv vrcholovému managementu.

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

Použijí se ustanovení této kapitoly. 5.10.1.

5.10.3 Postupy pro ohrožení soukromého klíče

Použijí se ustanovení této kapitoly. 5.10.1.

5.10.4 Kompromitace algoritmů

Pokud by se měl stát některý z algoritmů nebo souvisejících parametrů, které používá TSP nebo jeho Zákazníci nedostatečným pro jeho původně zamýšlené použití, pak TSP informuje všechny Zákazníky a Spoléhající se strany, se kterými má TSP smlouvu nebo jinou formu navázaných vztahů. Kromě toho musí TSP zpřístupnit tyto informace dalším Spoléhajícím se stranám. TSP naplánuje zrušení jakéhokoli dotčeného certifikátu.

5.10.5 Kontinuita podnikání po katastrofě

Použijí se ustanovení této kapitoly. 5.10.1.

5.11 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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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]

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.

[1] Popis řešení vzdáleného QSCD v. 1.0, Ardaco, a.s.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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. 1.3 a 2.

Veřejné klíče Držitelů Poskytovatelem není zveřejňováno, s výjimkou zveřejnění certifikátů s jejich výslovným souhlasem ve veřejném úložišti podle kapitoly. 2.

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.

Tabulka 1: Minimální délky klíče (bit):

Předmět	RSA	ECDSA
Poskytovatel	4096	-
Koncové entity	2048	256

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.

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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 CHAP. 6.1.6 a 6.1.7.

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

6.4 Aktivační údaje

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 (tento 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 certifikátu TSA

7.2.1 Položky certifikátu TSA

Pole	Hodnota
version	3
serialNumber	Jedinečné sériové číslo přidělené Poskytovatelem
signatureAlgorithm	sha256withRSAEncryption
issuer	Vystavitel certifikátu (CA)
validity	

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

notBefore	Začátek platnosti certifikátu (UTCTime)
notAfter	Vypršení platnosti certifikátu (UTCTime)
subject	Viz rozlišovací jméno.
subjectPublicKeyInfo	
algorithm	rsaEncryption
subjectPublicKey	Veřejný klíč subjektu
extensions	Viz Rozšíření certifikátů TSA
signature	Razítko zprostředkovatele certifikační autority

7.2.2 Rozlišující název certifikátu TSA

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.
commonName	Ano	Identifikace vydávající jednotky.
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].

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

7.3.1 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

7.3.2 Rozlišující název certifikátu respondéru OCSP

Pole	Povinný	Hodnota
countryName	Ano	Dvoumístný kód státu.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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].

7.3.3 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.

7.4 Profil kvalifikovaného certifikátu

7.4.1 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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

<table>
<tr><td>extensions</td><td>

7.4.2 Rozšíření. Vidět Rozlišovacie meno kvalifikovaného certifikátu pre webové sídla

Pole	Povinné	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	Ne	Zastaralé.
organizationalName	Ano	Název právnické osoby, jak je uveden v příslušném rejstříku.
organizationIdentifier	Ne (viz ale poznámky k hodnotě)	Identifikátor organizace, jak je uveden v příslušném rejstříku. V případě PSD2 certifikátů povinné - informace organizaci ve formátu podle ETSI TS 119 495.
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	PSČ

Rozšíření kvalifikovaného certifikátů

</td></tr>
<tr><td>signature</td><td>Razítko poskytovatele CA.</td></tr>
</table>

7.4.3 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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

serialNumber	Ne	Odkaz na totožnost fyzické osoby ve formátu dokumentu Systém dohledu nad kvalifikovanými službami vytvářejícími důvěru definovaný orgánem dohledu [3]. Existující seznam zpřesňujících znaků v Schématu dohledu rozšiřuje Poskytovatel následovně: - **Slovenská republika:** přebírá konvenci Slovenské národní certifikační autority (SNCA) podle Seznamu zpřesňujících znaků SNCA, který je zveřejněn na webovém sídle SNCA - **Česká republika:** přebírá konvenci podle informací a doporučení Digitální a informační agentury, Dokument upřesňující problematiku zápisu údajů o čísle dokladu do kvalifikovaného certifikátu, jmenovitě:[2] o IR - Povolení k pobytu/Pobytová karta/Karta trvalého pobytu s biometrickými údaji (forma: plastiková karta s čipem) o IX - Forma: knížečka (označení CIS: PB - povolení k pobytu, PE - průkaz o povolení k trvalému pobytu obč. EU, PO - průkaz o povolení k trv. pobytu - vazba EU, PP - průkaz o povolení k pobytu, PR - průkaz o pobytu rod. př. obč. EU - přech. pobyt)
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
userId	Ne	Interní identifikátor subjektu pro potřeby CA.

7.4.4 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

[2] Dokument (v0.1) nebyl v době tvorby CPS veřejně dostupný, proto kvůli jednoznačnosti jmenovitě uvádíme konkrétní používané položky.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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.

7.4.5 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 (viz ale poznámky k hodnotě)	Identifikátor organizace, jak je uveden v příslušném rejstříku. V případě PSD2 certifikátů povinné - informace organizaci ve formátu podle ETSI TS 119 495.
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	Psč

7.4.6 Rozlišovacie meno kvalifikovaného certifikátu pre webové sídla

Pole	Povinné	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	Ne	Zastaralé.
organizationalName	Ano	Název právnické osoby, jak je uveden v příslušném rejstříku.
organizationIdentifier	Ne (viz ale poznámky k hodnotě)	Identifikátor organizace, jak je uveden v příslušném rejstříku. V případě PSD2 certifikátů povinné - informace organizaci ve formátu podle ETSI TS 119 495.
organizationalUnitName	Ne	Název organizační jednotky
stateOrProviceName	Ne	Územní jednotka
localityName	Ne	Vesnice
streetAdress	Ne	Ulice
postalCode	Ne	PSČ

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

7.4.7 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, QEVCP-w 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 (viz ale poznámky k hodnotě)	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. 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-qcs-QcType s hodnotou podle příslušného typu certifikátu id-etsi-psd2_qcStatement - pro 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).

7.5 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)

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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.

7.6 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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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

7.7 Profil časového razítka

Profil žádosti a odpovědi musí být v souladu s [ETSI 319 422] a IETF RFC 3161. Hodnoty jsou konzistentní s definicí ve výše uvedeném dokumentu RFC a jsou explicitně uvedeny pouze v případě, že TSA očekává nebo vrátí konkrétní hodnotu.

7.7.1 Profil požadavku

Pole	Povinný	Hodnota
version	Ano	V1 (1)
messageImprint	Ano	Algoritmus OID pro výpočet otisku a otisku dat, která mají být orazítkována
reqPolicy	Ne	Je-li zadán, musí být identifikátor OID: 1.3.158.35829036.0.0.0.1.0 (Certifikační politika pro kvalifikovanou důvěryhodnou službu pro vytváření kvalifikovaných elektronických časových razítek)
nonce	Ne	
certReq	Ano	Výchozí hodnota false

7.7.2 Profil odpovědi

Pole	Povinný	Hodnota
status	Ano	Stav hovoru
timeStampToken	Ne	
contentType	Ano	id-ct-TSTInfo
content	Ano	
version	Ano	V1 (1)
policy	Ano	Vždy: OID: 1.3.158.35829036.0.0.0.1.0 (Certifikační politika pro kvalifikovanou důvěryhodnou službu pro vytváření kvalifikovaných elektronických časových razítek)

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

messageImprint	Ano	Vždy odpovídá stejné hodnotě v požadavku.
serialNumber	Ano	Jedinečné sériové číslo přidělené TSA
genTime	Ano	Čas od TSA
accuracy	Ano	max 1s
ordering	Ano	
nonce	Ne	Uvádí se, zda byla v žádosti uvedena hodnota Nonce – stejná hodnota.
tsa	Ne	Obecný název TSA
extensions	Ne	Nepoužívá se

8 Audit souladu a další hodnocení

Účelem auditu je potvrdit, že kvalifikovaný Poskytovatel důvěryhodných služeb a kvalifikované důvěryhodné služby, které poskytuje na základě této CPS, splňují požadavky stanovené nařízením eIDAS. Poskytovatel musí podstoupit audit alespoň každých 12 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. 1.3nebo 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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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

Tento CPS 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 CPS.

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.

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 i této 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 CPS 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:

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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 1.3. 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.

V případě oznamování důležitých změn v poskytování důvěryhodných služeb dozorčímu orgánu včetně změn v poskytování důvěryhodných služeb a záměru ukončit jejich poskytování v souladu s obchodními požadavky a příslušnými zákony a předpisy je TSP povinen informovat dozorový orgán:

a) jeden měsíc před provedením dané změny;
b) tři měsíce před plánovaným ukončením poskytování důvěryhodných služeb.

9.12 Novelizace

Postup novelizace této CPS 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 CPS 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

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s.
Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

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.

9.17 Dodatečné testování

Poskytovatel umožňuje třetím stranám zkontrolovat a otestovat všechny typy certifikátů, které vydává. V tomto kontextu může používat certifikáty vydané v produkčním prostředí.

Pokud se pro testování používají certifikáty vydané v produkčním prostředí, takové produkční certifikáty musí být v souladu s platnou Certifikační politikou. Takové testovací certifikáty nemohou být použity nad rámec testování a jsou jednoznačně označeny:

c) v názvu subjektu příponou ,,TEST”
d) atribute nsComment jednoznačným popisem, že jde o testovací certifikát, pokud to není vzhledem k povaze a účelu testování technicky možné uvést podle bodu a)

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.

10 Odkazy

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce 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 důvěryhodných službách pro elektronické obchody na vnitřním trhu a o změně některých zákonů (zákon o důvěryhodných službách)

[3] Systém dohledu nad kvalifikovanými službami vytvářejícími důvěru definovaný orgánem dohledu v1.4 – 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 důvěryhodných službách, 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 důvěryhodných službách 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 důvěryhodných službách vydávající certifikáty; Část 2: Požadavky na poskytovatele důvěryhodných službách 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] CP, Certifikační politika pro KC a Certifikační politika pro ČP , Certifikační politika pro KC a ČP
Certifikační politika Ardaco pro služby vyhotovování a ověřování kvalifikovaných certifikátů
Certifikační politika Ardaco pro služby vyhotovování a ověřování kvalifikovaných certifikátů (CZ verze)
Certifikační politika pro kvalifikovaná časová razítka
Certifikační politika Ardaco poskytování kvalifikované důvěryhodné služby validace KEP a KEPe

[15] Popis řešení Remote QSCD – interní dokument

[16] Pravidla pro výkon certifikačních činností (CPS)
Pravidla pro výkon certifikačních činností (CPS) Ardaco

[17] 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

[18] CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates, .

[19] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers;

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

[21] Pravidlá na výkon SSAS Ardaco a Pravidla pro výkon SSAS Ardaco (CZ verze)

Ardaco, a.s. © 2023-2026
Pravidla pro výkon certifikačních činností (CPS) Ardaco je veřejný dokument, který je majetkem společnosti Ardaco, a.s. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu vlastníka autorských práv.