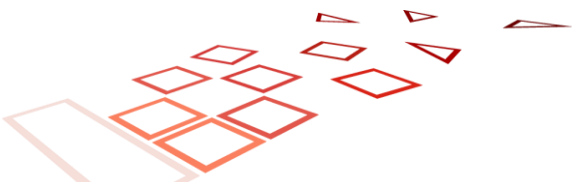
ARDACO
DATA & COMMUNICATION SECURITY

Vyhlásenie o zverejnení PKI
(PKI Disclosure Statement)

ver. 1.0

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	31.8.2023	Richard Margala	Prvá verzia dokumentu.



1 Úvod

Vyhlásenie o zverejnení PKI (Public Key Infrastructure Disclosure Statement) slúži na informovanie užívateľov a zákazníkov o politike a postupoch poskytovateľa certifikačných služieb pri správe infraštruktúry verejných kľúčov (PKI). Tento dokument, vytvorený v súlade s normou ETSI EN 319 411-1, poskytuje prehľad o zásadách bezpečnosti, zodpovednostiach strán a súlade s právnymi požiadavkami.

Cieľom vyhlásenia je zabezpečiť transparentnosť procesov PKI, čím sa posilňuje dôvera užívateľov v elektronické transakcie a komunikáciu. Umožňuje lepšie pochopiť, ako poskytovateľ certifikačných služieb chráni integritu a dôvernosť digitálnych certifikátov, ktoré sú kľúčové pre ochranu citlivých informácií v digitálnom prostredí.

2 Kontaktné údaje

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

3 Typy certifikátov, postupy overenia a použitie

3.1 Typy certifikátov

Ardaco (ďalej aj ,,Poskytovateľ") poskytuje certifikáty podľa normy ETSI 319 411 a súvisiacich štandardov.

Certifikačná autorita **Ardaco QSCA** vydáva certifikáty pre fyzické osoby a právnické osoby, ako je definované v Certifikačnej politike / Certifikačnej prevádzkovej smernici.

Vydávané sú nasledovné typy kvalifikovaných certifikátov:

Typ	Popis	Účel
QCP-n	Kvalifikovaný certifikát pre fyzickú osobu	Zdokonalený elektronický podpis
QCP-n-qscd	Kvalifikovaný certifikát pre fyzickú osobu vydaný na kvalifikované zariadenie na vyhotovenie elektronického podpisu	Kvalifikovaný elektronický podpis
QCP-l	Kvalifikovaný certifikát pre právnickú osobu	Zdokonalená elektronická pečať
QCP-l-qscd	Kvalifikovaný certifikát pre právnickú osobu	Kvalifikovaná elektronická pečať

	vydaný na kvalifikované zariadenie na vyhotovenie elektronického podpisu	

Podrobné profily certifikátov sú zverejnené v Certifikačnej prevádzkovej smernici.

Okrem kvalifikovaných certifikátov koncových používateľov je Ardaco QSCD vydávajúcou certifikačnou autoritou pre certifikáty využívané pri poskytovaní vlastných kvalifikovaných dôveryhodných služieb:

- **Ardaco OCSP Signer:** OCSP služba pre overovanie kvalifikovaných certifikátov pre elektronický podpis a pečať
- **Ardaco TSA:** služa kvalifikovanej časovej pečiatky
- **Ardaco Qualified Validation Service 1:** validácia kvalifikovaných elektronických podpisov a pečatí

Všetky certifikáty služieb pre poskytovanie kvalifikovaných dôveryhodných služieb sú dostupné na stránke https://tsp.ardaco.com.

3.2 Postupy overenia

Ardaco pri vydávaní kvalifikovaného certifikátu vhodnými prostriedkami a v súlade s vnútroštátnym právom overuje totožnosť a prípadne akékoľvek osobitné atribúty fyzickej alebo právnickej osoby, ktorej vydáva kvalifikovaný certifikát.

Overenie identity fyzickej osoby je možné jedným z nasledovných spôsobov:

a) preukázaním sa primárnym a sekundárnym dokladom
b) podpisom kľúčom, ktorý patrí kvalifikovanému certifikátu, pričom tento pôvodný kvalifikovaný certifikát
   - bol vydaný Poskytovateľom, čím nie je dotknutá povinnosť Poskytovateľa overiť aktuálnosť údajov, alebo
   - ide o kvalifikovaný certifikát vydaný na elektronický občiansky preukaz s čipom podľa § 4 Zákona č 395/2019 Z. z. o občianskych preukazoch a o zmene a doplnení niektorých zákonov a Poskytovateľ overí živosť osoby
c) preukázaním sa primárnym dokladom a záznamom o vykonaní kontroly aktuálnosti údajov voči spoľahlivému zdroju (napr. Register fyzických osôb, Registr obyvatel) a to najmä v prípade, že je registračnou autoritou banka, pričom bola osoba identifikovaná v zmysle AML predpisov (...)

Pri mandátnych certifikátoch sa oprávnenie konať preukazuje podľa zoznamu dokladov, ktoré sú pre dané oprávnenie uvedené v zozname oprávnení podľa § 9 zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

V prípade certifikátu pre právnickú osobu overuje identitu právnickej osoby a akýchkoľvek špecifických atribútov, ktoré sú uvádzané v certifikáte buď:

a) fyzickou prítomnosťou oprávneného zástupcu alebo
b) metódami, ktoré poskytujú rovnaký stupeň záruk ako fyzická prítomnosť oprávneného zástupcu

Na overenie identity právnickej slúži výpis z registra, v ktorom je daná právnická osoba evidovaná (napr. Obchodný register, Živnostenský register, Register neziskových organizácií a pod).

Podrobnosti, vrátane zoznamu akceptovaných dokladov, sú uvedené v Certifikačnej prevádzkovej smernici (CPS).

3.3 Použitie certifikátov

Kvalifikované certifikáty je možné používať iba v súlade s platnými právnymi predpismi a za podmienok, ktoré sú definované v Certifikačnej politike (CP), Certifikačnej prevádzkovej smernici (CPS) a Všeobecných obchodných podmienkach (VOP). Akékoľvek iné použitie je zakázané

4 Spoľahlivosť

Kvalifikovaný certifikát smie byť použitý iba na podpis alebo pečať.

Doba, počas ktorej sú uchovávané registračné informácie a záznamy udalostí Poskytovateľa dôveryhodných služieb je min. 10 rokov.

5 Povinnosti predplatiteľa

Predplatiteľ (alebo aj ,,Zákazník") je osoba alebo organizácia, ktorá žiada o vydanie certifikátu od certifikačnej autority (CA) a zodpovedá za akceptovanie podmienok použitia certifikátu.

Držiteľ certifikátu je fyzická alebo právnická osoba, ktorá je uvedená ako subjekt v certifikáte.

Predplatiteľ môže byť priamo Držiteľom certifikátu, alebo v prípade certifikátu vydaného pre právnickú osobu, môže byť Predplatiteľom organizácia, ktorá potom určí Držiteľa certifikátu (napríklad zamestnanca).

Povinnosti Držiteľa a Predplatiteľa sú uvedené v Zmluve o vydaní a používaní kvalifikovaného certifikátu.

Predplatiteľ je v každom prípade povinný najmä:

a) pri registrácii žiadosti o vydanie certifikátu uvádzať pravdivé a úplné údaje;
b) skontrolovať, či sú údaje uvedené v žiadosti o certifikát a v samotnom certifikáte správne a zodpovedajú požadovaným;
c) bezodkladne informovať Poskytovateľa o zmenách údajov uvedených vo vydanom certifikáte, resp. v zmluve;
d) dodržiavať všetky ustanovenia CPS, Zmluvy o poskytovaní Služby a legislatívy pre dôveryhodné služby, ktoré sa vzťahujú k povinnostiam Predplatiteľa

Držiteľ je v každom prípade povinný najmä:

a) používať súkromný kľúč a certifikát iba na účel, na ktorý bol určený
b) dodržiavať všetky ustanovenia CPS, Zmluvy o poskytovaní Služby a legislatívy pre dôveryhodné služby, ktoré sa vzťahujú k povinnostiam Držiteľa
c) zabrániť neoprávnenému použitiu súkromného kľúča
d) bezodkladne informovať Poskytovateľa o skutočnostiach, ktoré vedú k zneplatneniu certifikátu, predovšetkým stratu, podozrenie s neoprávneného použitia súkromného kľúča alebo kompromitáciu prístupových údajov
e) pri kompromitácii súkromného kľúča okamžite ukončiť jeho používanie

6 Kontrola stavu certifikátu spoliehajúcimi sa stranami

Spoliehajúce sa strany (každý, kto sa spolieha na informácie obsiahnuté v certifikáte) musia:

a) overiť platnosť, alebo zrušenie certifikátu pomocou aktuálnych informácií o jeho zrušení
b) zohľadniť akékoľvek obmedzenia používania certifikátu uvedené pre spoliehajúcu sa stranu buď v certifikáte, alebo vo Všeobecných podmienkach
c) prijať akékoľvek ďalšie opatrenia predpísané v dohodách alebo inde.

Za účelom overenia platnosti certifikátu obsahuje každý certifikát koncového používateľa adresu zoznamu zrušených certifikátov (CRL) a adresu služby Online Certificate Status Protocol (OCSP).

7 Obmedzenie záruk a zodpovednosti

Poskytovateľ zodpovedá v zmysle čl. 13 Nariadenia eIDAS výhradne za škodu, ktorú spôsobí úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplní svoje povinnosti podľa tohto Nariadenia.

Poskytovateľ nezodpovedá za vady poskytnutých služieb v prípade nesprávneho alebo neoprávneného využívania služieb poskytnutých na základe Zmluvy o poskytovaní služieb držiteľom certifikátu, najmä, nie však výlučne za využívanie služieb v rozpore s podmienkami poskytovania služieb.

Ďalej nezodpovedá za nepriame alebo iné straty alebo škody, vrátane ušlého zisku, ktoré môžu vzniknúť zákazníkom, držiteľom certifikátov, spoliehajúcim sa stranám alebo akýmkoľvek tretím stranám z dôvodu pôsobenia vyššia moci a ďalších vymenovaných v CPS.

Poskytovateľ nezodpovedá za škody, ktoré vznikli spoliehajúcej sa strane z dôvodu, že pri spoliehaní sa na certifikát a dôveryhodné služby Poskytovateľa, resp. na elektronický podpis alebo pečať vyhotovené na ich základe nepostupovala v zmysle CP a CPS.

8 Aplikovateľné dohody, CPS, CP

Vzťah medzi Predplatiteľom a Poskytovateľom sa okrem ustanovení príslušných právnych predpisov riadi zmluvou a ustanoveniami platnej CP, CPS a VOP.

Vzťah medzi Spoliehajúcou stranou a Poskytovateľom nie je upravený zmluvou a riadi sa príslušnými ustanoveniami platnej CP a CPS.

Všetky verejné informácie možno získať na adrese https://tsp.ardaco.com.

9 Zásady ochrany osobných údajov

Ochrana osobných údajov je riešená v súlade s platnou legislatívou týkajúcou sa osobných údajov t.j. zákonom Slovenskej republiky č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe týchto údajov a ktorou sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

10 Náhrada škody

Poskytovateľ nezodpovedá za škody spôsobené Zákazníkovi, Držiteľovi alebo spoliehajúcim sa stranám v prípade, ak bola škoda spôsobená v dôsledku a/ alebo v súvislosti s nesplnením povinností požadovaných právnymi predpismi pre dôveryhodné služby a touto CPS ako aj CP.

Poskytovateľ nezodpovedá za porušenie svojich povinností, ak bolo porušenie týchto povinností spôsobené vyššou mocou. Za vyššiu moc sa považuje najmä vojna, požiar, povodeň, veľké prírodné anomálie, prerušenie dopravy,

embargo, vládne opatrenia, pandémie, výbuch, ako aj dôsledok akýchkoľvek iných príčin, na ktoré Poskytovateľ nemá vplyv. Tieto okolnosti sú dôvodom k odkladu plnenia povinností na strane Poskytovateľa po dobu a v rozsahu účinnosti týchto okolností

11 Rozhodné právo, sťažnosti a riešenie sporov

Všetky spory, ktoré vznikli v súvislosti s výkonom dôveryhodnej služby Poskytovateľom budú riešené prioritne zmierovacím konaním medzi stranami sporu. Ak nedôjde k dohode o sporných nárokoch do 30 pracovných dní odo dňa uplatnenia nároku u druhej zmluvnej strany, ktorákoľvek zo strán je oprávnená podať žalobu na príslušný súd Slovenskej republiky. Súdy Slovenskej republiky sú vždy príslušné aj na prejednanie sporov s cudzím prvkom.

Vzťahy medzi Poskytovateľom a Zákazníkom/Držiteľom ako aj činnosť spoločnosti Ardaco a.s. sa spravujú právnym poriadkom Slovenskej republiky

12 TSP a úložisko, licencie, značky dôveryhodnosti a audit

Ardaco je akreditované ako kvalifikovaný poskytovateľ dôveryhodných služieb podľa nariadenia eIDAS a zapísané do Zoznamu kvalifikovaných poskytovateľov dôveryhodných služieb: https://eidas.ec.europa.eu/efda/tl-browser.

Poskytovanie týchto služieb je minimálne raz za 24 mesiacov podrobené posúdeniu zhody s príslušnými právnymi predpismi a technickými štandardami nezávislým Orgánom posudzovania zhody.

Zoznam získaných certifikátov:

Názov	Verzia	Platnosť od
Certifikát súladu s eIDAS pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis	-	22.07.2022
Certifikát súladu s eIDAS pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať	-	22.07.2022
Certifikát súladu s eIDAS pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických pečiatok	-	22.07.2022
Certifikát súladu s eIDAS pre kvalifikovanú dôveryhodnú službu validácie kvalifikovaných elektronických podpisov	-	22.07.2022
Certifikát súladu s eIDAS pre kvalifikovanú dôveryhodnú službu validácie kvalifikovaných elektronických pečatí	-	22.07.2022