ARDACO
DATA & COMMUNICATION SECURITY

Politika Ardaco

ver 1.0.5

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	12.10.2021	Richard Margala	Prvá verzia dokumentu.
1.0.1	16.12.2021	Richard Margala	Oprava chýb v terminológii (kapitola 6.1 Skratky)
1.0.2	3.3.2022	Richard Margala	Doplnenie aplikovania aj na nasledovné služby • Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov • Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí
1.0.3	30.5.2023	Richard Margala	Aktualizácia Mestského súdu a skrátenie názvu dokumentu
1.0.4	23.11.2023	Richard Margala	Zmena pojmu „Okresný súd Bratislava III“ na „Mestský súd Bratislava III“
1.0.5	30.3.2025	Richard Margala	Doplnenie pravidiel pre informačnej bezpečnosti pre dodávateľskú spoluprácu Politika používania cloudových služieb a riadenia súvisiacich bezpečnostných rizík

Obsah

1 Úvod

Tento dokument definuje politiku dôveryhodnej služby definovanej v kapitole 2 Účel spoločnosti Ardaco, a.s, so sídlom. Polianky 5, 841 01 Bratislava, zapísanej v Obchodnom registri Mestského súdu Bratislava III, v oddiely Sa, vložka číslo 2903/B.

Základný rámec pre poskytovanie dôveryhodných služieb tvoria:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (nariadenie eIDAS)
- Zákon č. 272/2016 Z.z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR
- Zákon č 69 z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

1.1 Názov dokumentu a jednoznačná identifikácia

Názov dokumentu a jednoznačná identifikácia	Politika Ardaco ver. 1.0.3
OID	Neudeľuje sa

1.2 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

2 Účel

Dôveryhodné služby v zmysle certifikačnej schémy orgánu dohľadu [4] ako aj nariadenia(EÚ) č. 910/2014 [5], ktoré sú organizáciou zabezpečované a popisované v certifikačnej politika:

1. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis
2. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať

3. Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov
4. Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí
5. Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre autentifikáciu webových sídiel

3 Skratky

CA	Certifikačná autorita
CRL	Zoznam zneplatnených certifikátov (Certification Revocation List)
KC	Kvalifikovaný certifikát
ČP	Časová pečiatka
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
RA	Registračná autorita

4 Pojmy

certifikačná autorita https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf

Dôveryhodná autorita, ktorá generuje certifikáty a zoznamy zrušených certifikátov (komponent infraštruktúry PKI). Kvalifikovanej dôveryhodnej služby vyhotovovania kvalifikovaných certifikátov podľa nariadenia (EÚ) č. 910/2014.
Rec. ITU-T X.509 [2] - 3.5.16 certification authority (CA): An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys.

certifikačné služby
Služby, ktoré poskytuje certifikačná autorita (registrácia, vydávanie certifikátu, overenie platnosti a funkčnosti certifikátu, zrušenie certifikátu, výmena kľúčov...).

certifikačná politika

Pomenovaný zoznam pravidiel, ktoré označujú použiteľnosť certifikátu v príslušnej skupine alebo triede aplikácií zdieľajúcej spoločné bezpečnostné požiadavky.

Rec. ITU-T X.509 [2] - 3.5.10 certificate policy: A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

certifikát

Reťazec údajov, ktorý spája identifikátor (Distinguished Name) subjektu s verejným kľúčom subjektu pomocou digitálneho podpisu. Formát tohto reťazca údajov je definovaný v Rec. ITU-T X.509 alebo ISO/IEC 9594-8. Tento reťazec údajov taktiež obsahuje identifikátor vydavateľa certifikátu, špecifické sériové číslo certifikátu, dobu platnosti a ďalšie údaje.

Rec. ITU-T X.509 [2] - 3.5.53 public-key certificate (PKC): The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the CA which issued it.

„certifikát pre elektronický podpis“ je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym;

„kvalifikovaný certifikát pre elektronický podpis“ je certifikát pre elektronický podpis, ktorý vydáva kvalifikovaný poskytovateľ dôveryhodných služieb a ktorý spĺňa požiadavky stanovené v prílohe I;

digitálny podpis

Digitálny podpis: údaje pripojené k alebo kryptografická transformácia dátovej jednotky, ktorá umožňuje príjemcovi dátovej jednotky preukázať zdroj a integritu dátovej jednotky a chrániť pred falšovaním napr. príjemcom

Odporúčanie ITU-T X.800 alebo ISO / IEC 7498-2 Rec. ITU-T X.509 [2] - 6.1 Digitálny podpis

Digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

Recommendation ITU-T X.800 alebo ISO/IEC 7498-2 Rec. ITU-T X.509 [2] - 6.1 Digital signature

registračná autorita

Entita primárne zodpovedná za identifikáciu a autentifikáciu subjektu certifikácie. Komponent infraštruktúry PKI používaný na posúvanie schválených žiadostí o vydanie certifikátu do certifikačnej autority.

Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly. This service includes proof of possession of non-CA generated subject private keys. Pozri IETF RFC 3647 [1] a Rec. ITU-T X.509 [2] schéma dohľadu Schému dohľadu kvalifikovaných dôveryhodných služieb definuje orgán dohľadu (NBÚ), pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf

spoliehajúca sa strana

Subjekt alebo komponent, ktorý požaduje od PKI infraštruktúry overenie stavu certifikátu. Rec. ITU-T X.509 [2] - 3.5.55

relying party: A user or agent that relies on the data in a certificate in making decisions

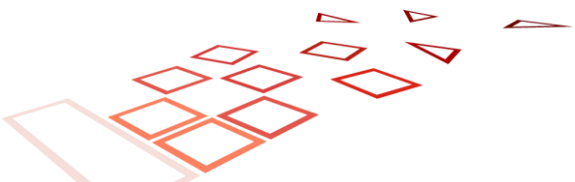
„spoliehajúca sa strana“ je fyzická osoba alebo právnická osoba, ktorá sa spolieha na elektronickú identifikáciu alebo dôveryhodnú službu; [8]

podpisovateľ [8]

fyzická osoba, ktorá vyhotovuje elektronický podpis;

dôveryhodná služba [8]

elektronická služba, ktorá sa spravidla poskytuje za odplatu a spočíva:



a) vo vyhotovovaní, overovaní a validácii elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo
b) vo vyhotovovaní, overovaní a validácii certifikátov pre autentifikáciu webových sídiel, alebo
c) v uchovávaní elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia;

kvalifikovaná dôveryhodná služba [8]

je dôveryhodná služba, ktorá spĺňa uplatniteľné požiadavky stanovené v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES;

5 Hodnotenie a posúdenie rizík (Risk Assesment)

Posúdenie rizika s cieľom identifikovať, analyzovať a vyhodnotiť riziká dôveryhodných služieb s prihliadnutím na obchodné a technické problémy je vykonávané na pravidelnej báze počas preskúmania manažmentom ,kedy sa vyhodnocujú všetky organizačné riziká.

Následne na to sa vyberú vhodné opatrenia na ošetrenie rizika s prihliadnutím na výsledky posúdenia rizika. Opatrenia na ošetrenie rizika zabezpečia, aby úroveň bezpečnosti bola primeraná stupňu rizika.

Pokyny k riadeniu rizík v oblasti bezpečnosti informácií ako súčasť systému riadenia bezpečnosti informácií je definovaný ako samostatný organizačný proces integrovaný v rámci Systému riadenia kvality podľa ISO 9001 s rozšírením o požiadavky podľa normy ISO 27001.

Taktiež boli určené všetky bezpečnostné požiadavky a prevádzkové postupy, ktoré sú potrebné na implementáciu definovaných opatrení na riešenie rizík, ako sú uvedené v politike bezpečnosti informácií a vyhlásení o postupoch dôveryhodných služieb. Hodnotenie rizika sa pravidelne prehodnocuje, zaznamená a reviduje, pričom manažmente organizácie schvaľuje hodnotenie rizika a identifikované zvyškové riziká.

6 Politiky a postupy (Policies and practices)

6.1 Vyhlásenie o postupoch dôveryhodnej služby (Trust Service Practice statement)

Organizácia definovala súbor politík a postupov vhodných pre dôveryhodné služby, ktoré poskytuje. Tieto sú schválené manažmentom organizácie, zverejnené a podľa potreby oznámené zamestnancom a externým stranám.

Vyhlásenia o službách dôveryhodnosti:

a) Organizácia má vyhlásenie o postupoch a procedúrach (statement of the practices and procedures, alebo Pravidlá na výkon certifikačných činností (CPS) Ardaco) používaných na splnenie všetkých požiadaviek určených v definovaných politikách pre KC ako aj ČP.
b) Organizácia má určené povinnosti všetkých externých organizácií podporujúcich služby vrátane príslušných politík a postupov.
c) Všetky požadované verejne publikované dokumenty na posúdenie súladu so zásadami služby (politiky, vyhlásenia a iné) sú publikované na stránke spoločnosti Ardaco, a.s. prístupné predplatiteľom ako aj zainteresovaným stranám.
d) Spoločnosť taktiež určila riadiaci orgán s celkovou zodpovednosťou za riadenie vyššie spomenutých služieb s konečnou právomocou schvaľovať vyhlásenia ako aj politiky.
e) Spoločnosť ako aj riadiaci orgán v maximálnej miere implementoval všetky požadované a potrebné postupy.
f) Proces preskúmania postupov a procedúr vrátane zodpovedností za udržiavanie vyhlásení je definovaný a integrovaný v rámci regulárnych procesov a postupov organizácie.
g) Všetky relevantné oznámenia o zmenách, ktoré sú plánované realizovať a majú dopad na TSP, sú schválené podľa písmena d) vyššie, taktiež sú revidované a publikované, ako sa vyžaduje v písmene c) vyššie.
h) Ukončenie dodávaných služieb je riadne riadené podľa zavedených postupov a procesov (viď odsek 7.12 Ukončenie TSP a plány ukončenia (TSP termination and termination plans)).

6.2 Zmluvné podmienky (Terms and Condition)

Organizácia sprístupnila podmienky týkajúce sa svojich služieb všetkým predplatiteľom a zainteresovaným stranám.

Tieto zmluvné podmienky definujú, že:

a) politika dôveryhodných služieb je zavedená do praxe;
b) akékoľvek obmedzenia týkajúce sa používania služby;
c) povinnosti predplatiteľa, ak existujú;
d) informácie pre zainteresované strany spoliehajúce sa na dôveryhodnú službu;
e) časové obdobie, počas ktorého sa uchovávajú protokoly;
f) obmedzenia zodpovednosti;
g) obmedzenia používania poskytovaných služieb vrátane obmedzenia škôd vzniknutých v dôsledku používania služieb presahujúcich tieto obmedzenia;
h) platný legislatívny základ;
i) postupy pre riešenie sťažností a urovnávanie sporov;
j) či bola dôveryhodná služba posúdená ako zhodná s politikou dôveryhodných služieb s definovanou schémou posudzovania zhody;
k) kontaktné informácie;

l) záväzky týkajúce sa dostupnosti.

Predplatitelia a zainteresované strany spoliehajúce sa na dôveryhodnú službu majú uzavretú zmluvu, kde sú definované a akceptované presné podmienky vrátane vyššie uvedených položiek.

Zmluvné podmienky sú publikované a verejne prístupné na verejnom webe sídla spoločnosti v elektronickej podobe a v ľahko zrozumiteľnom jazyku. Pri podpise sú aj v papierovej forme podpísané ako káže platná legislatíva.

6.3 Politika informačnej bezpečnosti (Information security policy)

Spoločnosť definovala aj politiku informačnej bezpečnosti, ktorá je schválená manažmentom spoločnosti so záväzkom jasného prístupu organizácie k riadeniu informačnej bezpečnosti. Zmeny v politike bezpečnosti informácií ja v prípade zmeny jasne publikovaná zainteresovaným stranám (predplatitelia, spoliehajúce sa strany, hodnotiace orgány, dozorné alebo iné regulačné orgány).

Organizácia taktiež zabezpečila, že:

a) Politika informačnej bezpečnosti je zdokumentovaná, implementovaná a udržiavaná vrátane definovaných bezpečnostných kontrol a prevádzkových postupov pre zariadenia, systémy a informačné aktíva poskytujúce služby. Politika informačnej bezpečnosti je zverejnená a pravidelne oznamovaná všetkým zamestnancom spoločnosti.
b) Organizácia sa zaviazala k plnej zodpovednosť za zhodu s postupmi predpísanými v politike bezpečnosti informácií, a to aj v prípade, ak nejaká funkčnosť je zabezpečovaná externými subjektami. Taktiež sa zaviazala k zodpovednosti za externé subjekty, pričom zabezpečí aj výkon kontrol vyžadovaných organizáciou aj externými subjektami.
c) Zásady informačnej bezpečnosti organizácie a súpis aktív pre informačnú bezpečnosť (viď kapitola 7.3 Správa majetku (Asset management)) je pravidelne prehodnocovaná počas preskúmania manažmentom spoločnosti a taktiež aj v prípade významných zmien, aby sa zabezpečila ich nepretržitá vhodnosť, primeranosť a účinnosť. Všetky zmeny, ktoré majú vplyv na úroveň poskytovanej bezpečnosti, sú schválené riadiacim orgánom.
d) Konfigurácie systémov sa pravidelne kontrolujú, či neobsahujú zmeny, ktoré porušujú bezpečnostné politiky.

6.3.1 Pravidla pre mobilnú bezpečnosť pre Držiteľa

V prípade, že dôveryhodné služby využíva držiteľ prostredníctvom mobilného telefónu, je rovnako dôležité dodržiavať niekoľko bezpečnostných pravidiel.

- ✓ Udržiavať svoje údaje v bezpečí, minimálne zapnutím bezpečnostných prvkov mobilného zariadenia (napr. nastavenie PIN kódu či odtlačok prstu pri odomknutí obrazovky. Neodporúča sa pre Android mobilné zariadenia, používať biometriu tváre.)
- ✓ Nikdy s nikým nezdieľajte svoje prístupové údaje. Svoj bezpečnostné kódy by sa mali naučiť; nenosiť ich zapísané nikde v blízkosti mobilného zariadenia. Prístupové údaje neukladať do mobilného zariadenia.
- ✓ Nenechávať svoje mobilné zariadenie bez dozoru
- ✓ Nesťahovať do mobilu čokoľvek z neznámeho zdroja
- ✓ Rôzne neoverené Java aplikácie, hry a pod. môžu zariadenie poškodiť.
- ✓ Využívať bezpečnú wifi sieť
- ✓ Nikdy sa nepripájať sa k neznámej (verejnej) wifi sieti a vždy používať sieť so zabezpečeným prístupom (WPA)
- ✓ Vypnúť si automatické pripájanie cez bluetooth

- ✓ Bluetooth a wifi zapínať vždy len v prípade potreby. Vždy sledovať, či mobilné zariadenie nekomunikuje s neznámymi zariadeniami.
- ✓ Pravidelne aktualizovať softvér
- ✓ Ak mobilné zariadenie využíva operačný systém s podporou aktualizácie softvéru, pravidelne ho aktualizovať, rovnako ako antivírový program.
- ✓ V prípade straty bezodkladne kontaktovať svojho mobilného operátora a požiadať o jej zablokovanie.

6.3.2 Pravidla pre informačnej bezpečnosti pre dodávateľskú spoluprácu

Povinnosti v oblasti informačnej bezpečnosti a SLA (Dohody o úrovni služieb) pre dodávateľskú spoluprácu:

- ✓ Dodávateľ je povinný mať aktuálnu, schválenú a zverejnenú politiku informačnej bezpečnosti.
- ✓ Dodávateľ je povinný dodržiavať tieto pravidlá v celom dodávateľskom reťazci, ak uzatvárajú subdodávateľské zmluvy na časti služieb IKT poskytovaných TSP.
- ✓ Dodávateľ je povinný mať určenú zodpovednú osobu za informačnú bezpečnosť.
- ✓ Dodávateľ je povinný poskytnúť meno, e-mailovú adresu a/alebo telefónne číslo tejto osoby.
- ✓ Dodávateľ je povinný mať preškolených zamestnancov v oblasti informačnej bezpečnosti.
- ✓ Práva správcu systému alebo „superužívateľa“ budú obmedzené na malý počet kvalifikovaných a autorizovaných osôb.
- ✓ Dodávateľ je povinný používať unikátne prístupové účty priradené konkrétnym osobám na kontrolu prístupu k údajom Ardaco,a.s. Nešpecifické účty (napr. servisné účty) musia byť neinteraktívne (t. j. používateľ sa na ne nemôže prihlásiť).
- ✓ Dodávateľ je povinný sa starať o informácie Ardaco, a.s v zmysle nariadenia 2016/679 GDPR (General Data Protection Regulation) alebo všeobecné nariadenie na ochranu osobných údajov.
- ✓ Dodávateľ je povinný mať zavedený a dokumentovaný postup riadenia incidentov, ktorý sa použije v prípade úniku údajov.
- ✓ Dodávateľ je povinný v prípade bezpečnostného incidentu alebo úniku údajov, ktorý má alebo môže mať vplyv na Ardaco,a.s., nahlásite podrobnosti do 24 hodín.
- ✓ Dodávateľ je povinný zabezpečiť vhodné opatrenia na zabezpečenie hesiel v spoločnosti – napr. predvolené systémové účty a účty administrátorov by mali byť premenované alebo deaktivované, ak je to možné. Heslá týchto účtov musia byť zmenené z predvolených hodnôt. Budete mať formálnu politiku správy hesiel, ktorá určuje minimálnu dĺžku hesla, požiadavky na jeho komplexnosť a dobu platnosti.
- ✓ Dodávateľ je povinný mať zavedené opatrenia na ochranu infraštruktúry pred malvérom a sieťovým narušením.
- ✓ Dodávateľ je povinný zabezpečiť bezpečnosť údajov prostredníctvom pravidelného penetračného testovania a testovania bezpečnosti softvéru pre klientov.

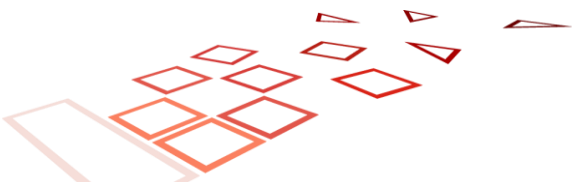
6.3.3 Politika používania cloudových služieb

Politika sa vzťahuje na všetky cloudové služby, ktoré využíva TSP na spracovanie, prenos alebo ukladanie dôverných, osobných, regulačne chránených alebo inak citlivých informácií. Vzťahuje sa aj na všetky tretie strany, ktoré sú do cloudových služieb zapojené.

Cloudové služby môže TSP využívať iba v prípade, že:

1. poskytovateľ služieb spĺňa štandardy ISO/IEC 27001 a/alebo iné relevantné bezpečnostné certifikácie (napr. CSA STAR, SOC 2),
2. sú jasne zadefinované pravidla zodpovednosti za bezpečnosť:

   a. TSP zodpovedá za:
      i. konfiguráciu cloudových služieb (napr. správne nastavenie prístupových práv, šifrovania),
      ii. kontrolu nad prenesenými alebo spracovávanými údajmi,
      iii. auditovanie a dohľad nad službami.
   b. Poskytovateľ cloudu je zodpovedný za:
      i. bezpečnosť infraštruktúry ako služby (IaaS), platformy (PaaS), alebo aplikácie (SaaS) podľa zmluvy,
      ii. fyzickú bezpečnosť dátových centier,
      iii. dostupnosť a údržbu služby.
3. lokalita dátových centier je známa a sú v súlade s GDPR a eIDAS.
4. sú publikované pravidlá ochrany osobných údajov
5. je zavedený dohľad nad bezpečnosťou cloudových služieb vrátane:
   a. monitorovania prístupov a podozrivých aktivít,
   b. pravidelného overovania konfigurácií
   c. logovania a archivácie auditných záznamov
6. v prípade spracovania dôverných alebo regulovaných údajov v cloude musí byť aktivované:
   a. šifrovanie údajov v prenose aj v pokoji
   b. viacfaktorová autentifikácia pre správcovské účty,
   c. zákaz verejného prístupu (public IP) mimo výnimiek.



7 Riadenie a prevádzka TSP (TSP management and operation)

7.1 Všeobecná vnútorná organizácia (Internal organization)

7.1.1 Spoľahlivosť (Organization reliability)

Organizácia, aby zabezpečila svoju spoľahlivosť tak, že:
a) zaviedla nediskriminačné postupy dôveryhodných služieb, podľa ktorých TSP funguje,
b) sprístupnila svoje služby všetkým žiadateľom, ktorých činnosť spadá do jej deklarovanej oblasti činnosti a ktorí sa zaväzujú dodržiavať svoje povinnosti uvedené v zmluvných podmienkach.
c) udržiava dostatočné finančné zdroj ako aj poistenie zodpovednosti v súlade s vnútroštátnym právom na krytie záväzkov vyplývajúcich z jej činností.
d) udržiava a plánuje svoje zdroje potrebné na prevádzku v súlade s touto politikou, aby udržiavala svoju stálu stabilitu
e) definovala politiky a postupy na riešenie sťažností a sporov prijatých od zákazníkov alebo iných zainteresovaných strán ohľadne poskytovania služieb alebo akýchkoľvek iných súvisiacich záležitostí.
f) zdokumentovala dohodu a zmluvný vzťah, v ktorom poskytovanie služieb zahŕňa subdodávky, outsourcing alebo iné dojednania s tretími stranami.

7.1.2 Rozdelenie povinností (Segregation of duties)

Organizácia plánuje svoje zdroje a pravidelne preskúmava ich rozdelenie, aby zabránila a minimalizovala konfliktné povinnosti a oblasti zodpovednosti. Zabezpečila ich oddelenie, aby sa znížila možnosť neoprávnených ako aj neúmyselných úprav či zneužitia aktív.

7.2 Ľudské zdroje (Human resources)

Ľudské zdroje predstavujú prioritný zdroj efektívnej činnosti s prosperity organizácie a v súčasnosti sú rozhodujúcim predpokladom budovania silných stránok a konkurenčných výhod organizácie.

Organizácia preto zabezpečila, aby organizačný personál, zamestnanci ako aj subdodávatelia:

a) pracovali len s potrebnými a vhodnými odbornými znalosťami a kvalifikáciu s vhodnými školeniami týkajúcich sa bezpečnosti informačných systémov ako aj zabezpečenia ochrany osobných údajov, tak aby boli dodávané len bezpečné služby s maximálnou mierou istoty.
b) boli schopní splniť požiadavku na odborné znalostí, skúseností a kvalifikácie prostredníctvom formálneho školenia a poverovacích listín, ako aj skutočných skúseností. Táto požiadavka, je taktiež pravidelne minimálne na preskúmaní manažmentom preverovaná so zabezpečením preverovania nových hrozieb a súčasných bezpečnostných postupoch.
c) pri porušení definovaných zásad alebo postupov organizácie sa uplatňoval disciplinárny proces a relevantné sankcie.
d) mal jasne identifikované, definované a zdokumentované úlohy a zodpovednosti v oblasti bezpečnosti, ktoré sú uvedené v politike bezpečnosti informácií, v popise práce ako aj v dokumentoch, ktoré sú publikované a prístupné na intranete organizácie. Dôveryhodné role boli riadne vymenované manažmentom organizácie a sú akceptované vedením a osobou na splnenie úlohy.

e) popisy pracovných miest bol definovaný tak aby bral ohľad na plnenú rolu s oddelením povinností, citlivosť údajov a úrovne prístupu, skríningu a školení.
f) vykonával administratívne a riadiace postupy a procesy v súlade s postupmi riadenia informačnej bezpečnosti.
g) mal požadované skúsenosti a školenia, nie len technického razenia ale aj skúsenosti a školenia týkajúce sa poskytovanej dôveryhodnej služby ako aj riadenia informačnej bezpečnosti (primárne sa to týka manažmentu spoločnosti),
h) nebol vystavení konfliktu záujmov, ktorý by mohol narušiť nestrannosť operácií
i) boli rozdelený do rolí: s nasledujúcimi zodpovednosťami:
    i. Bezpečnostní pracovníci: Celková zodpovednosť za správu implementácie bezpečnostných postupov.
    ii. Správcovia systému: Oprávnení na inštaláciu, konfiguráciu a údržbu dôveryhodných systémov organizácie na správu služieb.
    iii. Prevádzkovatelia systémov: Zodpovední za každodenné prevádzkovanie dôveryhodných systémov organizácie (oprávnenie na vykonávanie zálohovania systému).
    iv. Systémoví audítori: Oprávnení na prezeranie archívov a protokolov auditu dôveryhodných systémov organizácie (pre konkrétne dôveryhodné služby môžu byť požadované ďalšie role špecifické pre danú aplikáciu.)
j) personál organizácie je formálne menovaný do dôveryhodných rolí vrcholovým vedením zodpovedným za bezpečnosť, ktoré vyžaduje pri prístupe alebo pri konfigurácii prístupových oprávnení zásadu „najmenších privilégií“.
k) personál nemá prístup k dôveryhodným funkciám, kým sa nedokončia všetky potrebné kontroly či vo všetkých potrebných procesných krokoch je zabezpečená duálna kontrola.

7.3 Správa majetku (Asset management)

7.3.1 Všeobecné požiadavky (General requirements)

Organizácia zabezpečila primeranú a požadovanú úroveň ochrany svojich aktív vrátane informačných aktív čí aktív zameraných na ochranu osobných údajov.

Organizácia vypracovala inventarizáciu všetkých informačných aktív, ktorým taktiež pridelila klasifikáciu v súlade s hodnotením rizika. Organizácia , vo vypracovanej inventarizácii , identifikovala informácie, ako aj ďalšie aktíva spojené s informáciami a zariadeniami na spracovanie informácií a zabezpečila, že inventár týchto aktív je pravidelne aj udržiavaný a revidovaný.

7.3.2 Správa médií (Media handling)

So všetkými médiami sa manipuluje bezpečne v súlade s požiadavkami schémy klasifikácie informácií.
Médiá obsahujúce citlivé údaje sú bezpečne zneškodnené, ak už nie sú potrebné.

Organizácia implementovala základný proces pre manipuláciu s priradeným organizačnými médiami.

7.4 Riadenie prístupov (Access control)

Prístup do systémov organizácie je obmedzený len pre oprávnené osoby.

Sú implementované nasledovné procesné prvky:

a) Kontroly (napr. brány firewall) chránia vnútorné sieťové domény pred neoprávneným prístupom vrátane prístupu predplatiteľov a tretích strán. Brány firewall sú nakonfigurované tak, aby bránili všetkým protokolom a prístupom, ktoré nie sú potrebné na fungovanie organizácie.
b) Správa prístupov spravuje užívateľské prístupy operátorov, správcov a audítorov systému, pričom zabezpečuje manažment používateľských účtov a včasné informovanie o zmenách ako aj odstránení prístupu.
c) Správa prístupov spravuje prístupy k informáciám a funkciám aplikačného systému, ktoré sú obmedzené v súlade s politikou. Navrhnutý systém organizácie poskytuje dostatočné kontroly počítačovej bezpečnosti pre oddelenie dôveryhodných rolí identifikovaných v organizačných praktikách, procedúrach a postupoch vrátane oddelenia administrácie bezpečnosti a riadenia bežnej prevádzky. Obmedzené a kontrolované je aj použitie systémových obslužných programov.
d) Pracovníci organizácie sú menovaní, definovaní, identifikovaní a autentifikovaní pred použitím kritických aplikácií súvisiacich so službou.
e) Pracovníci organizácie zodpovedajú za svoju činnosť a ich činnosti sú zaznamenávané.
f) Citlivé údaje sú chránené pred odhalením (napr. obnova vymazaných súborov), v prípade ak je opätovne použitý ten isté úložné médiu , ak by bolo prístupné neoprávneným používateľom.

7.5 Kryptografické kontroly (Cryptographic controls)

Na účely správy všetkých kryptografických kľúčov a akýchkoľvek kryptografických zariadení počas celej ich životnosti sú zavedené vhodné bezpečnostné kontroly.

7.6 Fyzická a environmentálna bezpečnosť (Physical and environmental security)

Organizácia riadi fyzické prístupy ku komponentom podporovaných systémov, ktorých bezpečnosť je rozhodujúca pre poskytovanie dôveryhodných služieb, a minimalizuje riziká spojené s fyzickou bezpečnosťou.

Organizácia v plnej miere zabezpečuje

a) fyzické prístupy ku komponentom systému poskytujúceho dôveryhodné služby, ktorých bezpečnosť je kritická pre poskytovanie organizačných dôveryhodných služieb, je obmedzený na oprávnené osoby, pričom určenie kritickosti prístupov bola identifikovaná na základe posúdenia rizika ako aj na základe bezpečnostných požiadaviek aplikácie,
b) výkon zavedených kontrol, aby sa zabránilo strate, poškodeniu alebo zneužitiu majetku a prerušeniu obchodnej činnosti;
c) výkon zavedených kontroly, aby sa zabránilo kompromitácii alebo krádeži informácií a zariadení na spracovanie informácií;
d) uloženie komponentov, ktoré sú kritické pre bezpečnú prevádzku dôveryhodnej služby, v chránenom bezpečnostnom obvode s fyzickou ochranou pred narušením, kontrolami prístupu cez bezpečnostný obvod a poplachmi na detekciu narušenia.

Organizácia na zabezpečenia daných požiadaviek má implementovanú aj politiku čistého stola a obrazovky.

7.7 Prevádzková bezpečnosť (Operation security)

Organizácie používa dôveryhodné systémy a produkty, ktoré sú chránené proti zmene, a zaisťuje technickú bezpečnosť a spoľahlivosť nimi podporovaných procesov.

Organizácia zaviedla a dodržiava najmä tieto pravidlá:

a) Analýza bezpečnostných požiadaviek sa vykoná vo fáze návrhu a špecifikácie požiadaviek každého projektu vývoja systémov, ktorý uskutoční organizácia alebo v jeho mene, aby sa zabezpečilo zabudovanie bezpečnosti do IT systémov.
b) Na vydania, úpravy a núdzové opravy softvéru operačného softvéru a zmeny konfigurácie, ktoré uplatňujú bezpečnostnú politiku organizácie, sa uplatňujú postup riadenia zmien, pričom dané aktivity sú riadne zdokumentované, schválené ako aj komunikované zainteresovaným stranám.
c) Integrita systémov a informácií organizácie je chránená proti vírusom, škodlivému a neoprávnenému softvéru.
d) S médiami používanými v systémoch organizácie sa manipuluje bezpečne, aby sa chránili médiá pred poškodením, odcudzením, neoprávneným prístupom a zastaraním.
e) Postupy na správu médií chránia pred zastaraním a znehodnotením médií v období, počas ktorého sa vyžaduje uchovanie záznamov.
f) Organizácia má stanovené a zavedené postupy pre všetky dôveryhodné a administratívne úlohy, ktoré majú vplyv na poskytovanie služieb.
g) Organizácia špecifikovala a uplatňuje postupy na zabezpečenie:
h) použitie bezpečnostných záplaty v primeranej lehote po ich sprístupnení;
    i. nepoužitie bezpečnostných záplaty sa, ak spôsobujú ďalšie zraniteľnosti alebo nestability, ktoré prevažujú nad výhodami ich použitia;
    ii. zdokumentovanie dôvodov nepoužitia bezpečnostných záplat.

7.8 Sieťová bezpečnosť (Network security)

Organizácia chráni svoju sieť a systémy pred útokmi v maximálne možnej mier a to dodržiavaním nasledovných pravidiel:

a) Organizácia rozdelila svoje systémy na siete alebo zóny na základe posúdenia rizika s prihliadnutím na funkčný, logický a fyzický (vrátane umiestnenia) vzťah medzi dôveryhodnými systémami a službami. A taktiež uplatňuje rovnaké bezpečnostné kontroly na všetky systémy umiestnené v tej istej zóne.
b) Organizácia obmedzuje prístup a komunikáciu medzi zónami na tie, ktoré sú potrebné na prevádzku organizácie. Nepotrebné spojenia a služby sú výslovne zakázané a deaktivované. Stanovený súbor pravidiel sa pravidelne prehodnocuje.
c) Organizácia udržiava všetky systémy, ktoré sú kritické pre prevádzku, v jednej alebo viacerých zabezpečených zónach
d) Vyhradená sieť na správu IT systémov a operačnú sieť organizácie je oddelená. Systémy používané na správu implementácie bezpečnostnej politiky nie sú používané na iné účely. Produkčné systémy pre služby sú oddelené od systémov používaných pri vývoji a testovaní (napr. vývojové, testovacie a fázové systémy).
e) Komunikácia medzi odlišnými dôveryhodnými systémami sa uskutočňuje iba prostredníctvom dôveryhodných kanálov, ktoré sú logicky odlišné od ostatných komunikačných kanálov a poskytujú zaručenú identifikáciu jej koncových bodov a ochranu údajov kanála pred úpravami alebo zverejnením.
f) Ak sa vyžaduje vysoká úroveň dostupnosti externého prístupu k dôveryhodnej službe, externé sieťové pripojenie sú redundantné, aby sa zabezpečila dostupnosť služieb v prípade jedinej poruchy.
g) Organizácia vykonáva pravidelné skenovanie zraniteľnosti na verejných a súkromných identifikovaných IP adresách a zaznamenáva dôkazy o tom, že každé skenovanie zraniteľnosti bolo vykonané oprávnenou osobou, ktorá o tom vydáva aj samotnú správu.

h) Organizácia vykonáva penetračné skúšky v systémoch pri zriadení a po aktualizáciách alebo úpravách infraštruktúry alebo aplikácií, ktoré sú určené ako významné. Toto všetko je zaznamenané ako dôkazy o tom, že každý penetračný test sa vykonal osobou na to poverenou s požadovanými zručnosťami, nástrojmi, odbornosťou, etickým kódexom a nezávislosťou potrebnou na poskytnutie spoľahlivej správy.

7.9 Riadenie nezhôd (Incident management)

Organizácia monitoruje činnosti systému týkajúce sa prístupu do systémov IT, používania systémov IT a požiadaviek na služby.

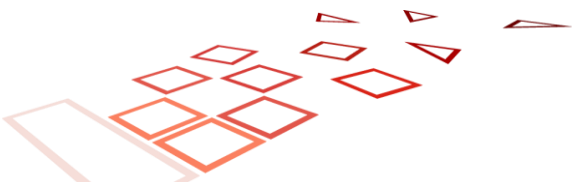
Organizácia dodržuje minimálne tieto pravidlá a postupu má definované v samostatnom organizačnom proces:

a) Monitorovacie činnosti berú do úvahy citlivosť akýchkoľvek zhromaždených alebo analyzovaných informácií.
b) Abnormálne činnosti systému , ktoré naznačujú potenciálne narušenie bezpečnosti, vrátane vniknutia do siete organizácie, sa zistia a nahlásia ((externé) sieťové kontroly alebo poklesy paketov) ako poplachy.
c) IT systémy organizácie monitorujú tieto udalosti:
    i. spustenie a vypnutie protokolovacích funkcií;
    ii. dostupnosť a využitie potrebných služieb so sieťou organizácie.
d) Organizácia koná včas a koordinovane, aby rýchlo reagoval na incidenty a obmedzila dopad narušení bezpečnosti. Vymenovala dôveryhodný personál, ktorý sleduje varovania o potenciálne kritických bezpečnostných udalostiach a zabezpečuje, aby sa príslušné incidenty hlásili v súlade s postupmi.
e) Organizácia stanovila postupy na informovanie príslušných strán v súlade s platnými regulačnými pravidlami o akomkoľvek narušení bezpečnosti alebo strate integrity, ktoré má výrazný vplyv na poskytovanú dôveryhodnú službu a na osobné údaje v nej uchovávané, do 24 hodín od zistené porušenie.
f) Organizácia informuje fyzickú alebo právnickú osobu aj o porušení bezpečnosti alebo strate integrity bez zbytočného odkladu, ak je narušenie bezpečnosti alebo strata integrity s nepriaznivým dopad na fyzickú alebo právnickú osobu, ktorej bola dôveryhodná služba poskytnutá.
g) Organizačné systémy sú monitorované vrátane monitorovania alebo pravidelného preskúmania protokolov auditu s cieľom identifikovať dôkazy o škodlivej činnosti pomocou automatických mechanizmov na spracovanie protokolov auditu a varovania personálu pred možnými kritickými bezpečnostnými udalosťami.
h) Organizácia pravidelne preveruje a rieši relevantnú kritickú zraniteľnosť do 48 hodín od jej zistenia. Ak je to vzhľadom na vplyv a náklady efektívne, Organizácia vytvorí a implementuje plán na zmiernenie zraniteľnosti a zdokumentuje vecný základ pre stanovenie, že zraniteľnosť nevyžaduje nápravu.
i) Postupy hlásenia a reakcie na incidenty sa používajú takým spôsobom, aby sa minimalizovali škody spôsobené bezpečnostnými incidentmi a poruchami.

7.10 Zbierka dôkazov (Collection of evidence)

Organizácia zaznamenáva a uchováva po primeranú dobu, aj po ukončení činnosti, všetky príslušné informácie týkajúce sa údajov vydaných a prijatých organizáciou, najmä na účely poskytovania dôkazov v súdnych konaniach a na účely účel zabezpečenia kontinuity služby.
Organizácia dodržuje minimálne tieto pravidlá:

a) Organizácia zachováva dôvernosť a integritu aktuálnych a archivovaných záznamov týkajúcich sa poskytovania služieb.
b) Záznamy týkajúce sa poskytovania služieb sa archivujú úplne a dôverne v súlade so zverejnenými obchodnými postupmi.
c) Záznamy týkajúce sa poskytovania služieb sa sprístupnia, ak sa to vyžaduje na účely preukázania správneho fungovania služieb na účely súdneho konania.



d) Záznamy obsahujú aj presný čas významných udalostí prostredia, správy kľúčov a synchronizácie hodín. Čas potrebný na zaznamenanie udalostí, sa synchronizuje v UTC najmenej raz denne.
e) Záznamy týkajúce sa služieb sa uchovávajú po dobu, ktorá je primeraná poskytnutiu potrebných právnych dôkazov a oznámené v podmienkach organizácie ako aj v bezpečnostnom projekte organizácie, ak sa týkajú osobných údajov.
f) Udalosti sa zaznamenávajú tak, aby ich nebolo možné ľahko vymazať alebo zničiť (okrem prípadov, ak sú spoľahlivo prenesené do dlhodobých médií) v časovom rozmedzí, v ktorom sa vyžaduje ich uskutočnenie.

7.11 Riadenie kontinuity činnosti (Business continuity management)

Organizácia definovala, implementovala, pravidelne preskúmava a udržiava plán kontinuity, ktorý prijala pre prípad katastrofy (napr. zlyhanie kritických komponentov dôveryhodného systému organizácie vrátane hardvéru a softvéru).

V prípade katastrofy, vrátane ohrozenia súkromného podpisového kľúča alebo ohrozenia nejakého iného poverenia organizáciou, sa operácie obnovia v rámci oneskorenia stanoveného v pláne kontinuity, pričom sa zabezpečí vyriešenie akejkoľvek príčiny katastrofy, ktorá by sa mohla opakovať (napr. zraniteľnosť bezpečnosti) s príslušnými nápravnými opatreniami.

7.12 Ukončenie TSP a plány ukončenia (TSP termination and termination plans)

V dôsledku ukončenia služieb organizácie sa minimalizujú potenciálne prerušenia predplatiteľov a spoliehajúcich zabezpečením nepretržitej údržby informácií potrebných na overenie správnosti dôveryhodných služieb, ako aj zabezpečením a dodržiavaním nasledovných pravidiel:

a) Organizácia vytvorí a pravidelne bude aktualizovať plán ukončenia v prípade ukončenia, rozhodnutie bude schválené manažmentom.
b) Ukončenie poskytovania dôveryhodných služieb bude vykonané s dodržaním nasledovných pravidiel:
    i. Organizácia informuje o ukončení nasledovné zainteresované strany: účastníkov a iné subjekty, s ktorými má uzavreté dohody alebo iné formy nadviazaných vzťahov, medzi ktorými sú relevantné autority a príslušné orgány. Tieto informácie sa navyše sprístupnia ďalším spoliehajúcim sa stranám;
    ii. Organizácia ukončí oprávnenie všetkých subdodávateľov konať v mene TSP pri výkone akýchkoľvek funkcií týkajúcich sa procesu vydávania tokenov dôveryhodných služieb
    iii. Organizácia prevedie povinnosti na spoľahlivú stranu, ktorá uchováva všetky informácie potrebné na zabezpečenie dôkazov o fungovaní organizácie po primeranú dobu, pokiaľ nie je možné preukázať, že organizácia takéto informácie nedrží;
    iv. Súkromné kľúče vrátane záložných kópií budú zničené a stiahnuté z používania takým spôsobom, že súkromné kľúče nebude možné získať;
    v. Pokiaľ je to možné, organizácia prijme opatrenia na prevod poskytovania dôveryhodných služieb pre svojich existujúcich zákazníkov na inú organizáciu.
c) Organizácie zabezpečí dohodu na pokrytie nákladov na splnenie týchto minimálnych požiadaviek v prípade, že skrachuje alebo z iných dôvodov nie je schopná pokryť náklady sama, pokiaľ je to možné v rámci obmedzení platných právnych predpisov týkajúcich sa bankrotu.
d) Organizácia vo svojich postupoch uviedla ustanovenia prijaté pre ukončenie služby, čo zahŕňa:
    i. oznámenie dotknutých subjektov;
    ii. prevod povinností organizácie na iné strany.

e) Organizácia zabezpečí činnosti prevádzania na spoľahlivú stranu svoje povinnosti týkajúce sa sprístupnenia jej verejného kľúča alebo jej tokenov dôveryhodných služieb spoliehajúcim sa stranám na primerané obdobie.

7.13 Súlad (Compliance)

Organizácia zabezpečila, aby fungovala legálnym a dôveryhodným spôsobom. Organizácia poskytuje dôveryhodné služby s platnými právnymi predpismi EU a Slovenskej republiky ako i príslušnými medzinárodnými štandardmi.

Organizácia dodržuje minimálne tieto pravidlá:

a) Organizácie poskytuje dôkazy o tom, ako spĺňa príslušné právne požiadavky.
b) Poskytované dôveryhodné služby a produkty koncových používateľov použité pri poskytovaní týchto služieb sa sprístupnia osobám so zdravotným postihnutím.
c) Prijíma príslušné technické a organizačné opatrenia proti neoprávnenému alebo nezákonnému spracovaniu osobných údajov a proti náhodnej strate alebo zničeniu alebo poškodeniu osobných údajov.

8 Orgán dohľadu

Poskytovateľ je povinný pri komunikácii s orgánom dohľadu postupovať v zmysle požiadaviek Nariadenia eIDAS [8] a Zákona o dôveryhodných službách [7].

Organizácia ako poskytovateľ dôveryhodných služieb poskytuje ako kvalifikované len tie dôveryhodné služby, na ktoré mu bol orgánom dohľadu udelený kvalifikovaný štatút.

Kvalifikovaný poskytovateľ dôveryhodných služieb podľa zákona 272/2016 Z. z. a v znení neskorších predpisov o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) je plne v súlade:

§ 3

(1) Poskytovateľ dôveryhodných služieb bez kvalifikovaného štatútu predkladá úradu oznámenie o zámere poskytovať kvalifikované dôveryhodné služby elektronickým formulárom alebo v listinnej podobe na tlačive, ktorého vzor zverejní úrad na ústrednom portáli verejnej správy a na svojom webovom sídle. K oznámeniu o zámere poskytovať kvalifikované dôveryhodné služby sa prikladajú certifikáty príslušnej kvalifikovanej dôveryhodnej služby, ktoré sa po udelení kvalifikovaného štatútu zaraďujú do dôveryhodného zoznamu.
(2) Kvalifikovaný poskytovateľ dôveryhodných služieb poskytuje ako kvalifikované len tie dôveryhodné služby, na ktoré mu je udelený kvalifikovaný štatút.
(3) Kvalifikovaný poskytovateľ dôveryhodných služieb, na ktorého dôveryhodnú službu úrad udelil kvalifikovaný štatút, uvádza vo vydanom kvalifikovanom certifikáte minimálne identifikátory certifikačných politík pre kvalifikované dôveryhodné služby vydávania kvalifikovaného certifikátu, ktoré úrad zverejní na svojom webovom sídle; certifikačné politiky obsahujú aj technické podmienky a postupy podpisovateľa a pôvodcu pečate.

§ 4

(1) Kvalifikovaný poskytovateľ dôveryhodných služieb môže autorizovať inú vlastnú kvalifikovanú dôveryhodnú službu alebo kvalifikovanú dôveryhodnú službu iného kvalifikovaného poskytovateľa dôveryhodných služieb na poskytovanie informácie o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov, ktoré vydal. Informácia o autorizácii podľa prvej vety sa uvedie v dôveryhodnom zozname vedenom úradom. Autorizácia platí, pokým ju autorizujúci kvalifikovaný poskytovateľ dôveryhodnej služby nezruší alebo pokým dôveryhodná služba nestratí kvalifikovaný štatút.

(2) Kvalifikovaný poskytovateľ dôveryhodných služieb môže pre prípad ukončenia poskytovania svojej kvalifikovanej dôveryhodnej služby uzavrieť zmluvu s iným kvalifikovaným poskytovateľom dôveryhodných služieb o poskytovaní informácie o štatúte platnosti alebo zrušenia vydaných kvalifikovaných certifikátov18) a prevzatí súvisiacej prevádzkovej dokumentácie. Ak kvalifikovaný poskytovateľ dôveryhodných služieb neuzavrel dohodu podľa prvej vety a nemá právneho nástupcu, poskytovanie informácie o štatúte platnosti alebo zrušenia vydaných kvalifikovaných certifikátov a prevzatie súvisiacej prevádzkovej dokumentácie zabezpečí úrad. V prípadoch podľa druhej vety dôjde k zrušeniu platných prevzatých kvalifikovaných certifikátov kvalifikovaným poskytovateľom dôveryhodnej služby, alebo ak to technicky nie je možné, tak úradom v prevzatej databáze certifikátov. Informácia o postupe podľa tohto odseku sa uvedie v dôveryhodnom zozname vedenom úradom.

§ 5

Kvalifikovaný poskytovateľ dôveryhodných služieb najmenej počas desiatich rokov uchováva informácie,

a) ktoré súvisia s vydaním a zrušením kvalifikovaných certifikátov od uplynutia platnosti kvalifikovaného certifikátu alebo zrušenia kvalifikovaného certifikátu spolu s vydaným kvalifikovaným certifikátom a informáciou o štatúte platnosti alebo zrušenia kvalifikovaného certifikátu aktualizovanou po uplynutí platnosti kvalifikovaného certifikátu alebo zrušení kvalifikovaného certifikátu,
b) na základe ktorých poskytoval kvalifikovanú dôveryhodnú službu; kvalifikovaný poskytovateľ dôveryhodných služieb uchováva tieto informácie od ich vzniku.

§ 6

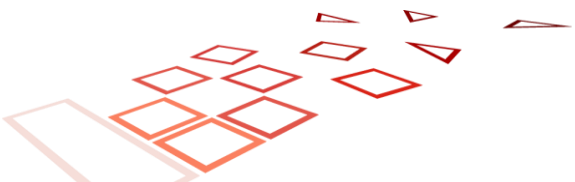
(1) Kvalifikovaný poskytovateľ dôveryhodných služieb poskytuje úradu informácie o zmenách v jeho kvalifikovaných dôveryhodných službách najneskôr do 30 dní pred plánovanou zmenou.
(2) Kvalifikovaný poskytovateľ dôveryhodných služieb, ktorému úrad udelil kvalifikovaný štatút, zasiela úradu
   a) vydané kvalifikované certifikáty pre kvalifikovaný elektronický podpis a pre kvalifikovanú elektronickú pečať do 30 dní od vydania kvalifikovaného certifikátu,
   b) po zrušení certifikátov podľa písmena a) potvrdenie o dátume a čase ich zrušenia do 30 dní od ich zrušenia,
   c) informáciu o ukončení používania údajov na vyhotovenie elektronického podpisu alebo elektronickej pečate kvalifikovanej dôveryhodnej služby, ktoré zodpovedajú údajom na validáciu elektronického podpisu alebo elektronickej pečate z certifikátov uvedených pre túto službu v dôveryhodnom zozname do 30 dní od ukončenia používania týchto údajov; to neplatí, ak dátum a čas konca platnosti posledného certifikátu uvedeného pre túto službu v dôveryhodnom zozname je zhodný s dátumom a časom ukončenia používania údajov na vyhotovenie elektronického podpisu alebo elektronickej pečate.
(3) Informácie podľa odsekov 1 a 2 sa predkladajú úradu elektronickým formulárom alebo v listinnej podobe na tlačive, ktorého vzor zverejní úrad na ústrednom portáli verejnej správy a na svojom webovom sídle.

§ 7

(1) Kvalifikovaný poskytovateľ dôveryhodnej služby, ktorý vydáva kvalifikované certifikáty, pri poskytovaní informácie o štatúte platnosti alebo zrušení kvalifikovaných certifikátov poskytuje aj informáciu obsahujúcu potvrdenie o dátume a čase, do ktorého boli certifikáty evidované ako platné, alebo informáciu o dátume a čase zrušenia kvalifikovaného certifikátu.
(2) Kvalifikovaný poskytovateľ dôveryhodných služieb, ktorému kvalifikovaný štatút udelil úrad, nesmie dočasne pozastaviť kvalifikovaný certifikát pre elektronický podpis alebo kvalifikovaný certifikát pre elektronickú pečať.

§ 12 Kontrola a dohľad

(2) Na účely výkonu kontroly má poskytovateľ dôveryhodných služieb práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.



9 Referencie

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

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

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

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32014R0910

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

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

[8] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R0910

[9] Certifikačná Politika pre KC

[10] Certifikačná Politika pre ČP

[11] Pravidlá na výkon certifikačných činností (CPS)