Č. p.:

DKDS1 Politika poskytovania dôveryhodných služieb NASES

Názov dokumentu:	DKDS1 Politika poskytovania dôveryhodných služieb NASES		
Označenie dokumentu:	DKDS1 Politika TSP NASES.pdf		
Verzia:	0.9	Status:	*Návrh*
Dátum vytvorenia:	18.11.2020	Platný do:	31.12.2021

História dokumentu

História revízií dokumentu

Verzia	Dátum	Popis zmeny	Autor / Autor zmien
0.9	18.11.2020	Úvodná verzia	Ing. Marián Štefánek

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

[1] ETSI EN 319 401 v.2.2.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (ďalej aj „Štandard TSP“).
Štandard TSP

[2] 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 (ďalej aj „Nariadenie eIDAS“).
Nariadenie eIDAS

[3] ISO/IEC 27005:2011 - "Information technology - Security techniques - Information security risk management" (ďalej aj „Štandard RM“).

[4] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (ďalej aj „Zákon o DS“).
Zákon č. 272/2016 Z. z. o dôveryhodných službách

[5] 05968/2019/ORD-001 - Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu, Verzia 1.4, Národný bezpečnostný úrad.
Schéma dohľadu KDS definovaná orgánom dohľadu

[6] Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad, Verzia 4.0, Kapitola 10, Národný bezpečnostný úrad.
Certifikačná politika pre KCA

Zoznam tabuliek

Tabuľka 1 Použité definície 5

Tabuľka 2 Použité skratky 5

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Dôveryhodná služba	Elektronická služba pre: • vyhotovovanie, overovanie a validáciu elektronických podpisov, elektronických pečatí alebo elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo; • vyhotovovanie, overovanie a validácia certifikátov pre autentifikáciu webových sídiel; alebo; • uchovávanie elektronických podpisov, pečatí alebo certifikátov prislúchajúcich týmto službám.
Odberateľ	Odberateľ kvalifikovaných dôveryhodných služieb poskytovaných agentúrou NASES.
Orgán dohľadu	Orgán zriadený na území členského štátu, ktorý je zodpovedný za úlohy dohľadu v určujúcom členskom štáte - v zmysle Zákona o DS, § 11, písm. a) je to v Slovenskej republike Národný bezpečnostný
Popis práce	Popis pracovných činností pracovníkov Poskytovateľa.
Poskytovateľ	Národná agentúra pre sieťové a elektronické služby.
Pracovník Poskytovateľa	Zamestnanec NASES.
Prevádzkovateľ	Organizačný útvar, ktorý na základe rozhodnutia Poskytovateľa prevádzkuje IS KDS.
Spoliehajúca sa strana	Fyzická alebo právnická osoba, spoliehajúca sa na elektronickú identifikáciu alebo dôveryhodnú službu.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
CA	Certifikačná autorita.
HW	Hardvér.
IS KDS	Informačný systém Kvalifikovaných dôveryhodných služieb Národnej agentúry pre sieťové a elektronické služby.
IT	Informačné technológie.
NASES	Národná agentúra pre sieťové a elektronické služby.
SNCA	Slovenská národná certifikačná autorita - certifikačná autorita, prevádzkovaná Národnou agentúrou pre sieťové a elektronické služby.
SW	Softvér.

Použité pojmy sú prevzaté z Nariadenia eIDAS [2] a Štandardu TSP [1].

Obsah

1	**Úvod**	**7**
1.1	Identifikácia dokumentu	7
2	**Všeobecné ustanovenia**	**8**
3	**Posúdenie rizík**	**9**
4	**Politiky a praktiky**	**10**
4.1	Politiky a pravidlá pre poskytovanie dôveryhodných služieb	10
4.2	Všeobecné podmienky	10
4.3	Politika informačnej bezpečnosti	11
5	**Riadenie a prevádzka dôveryhodných služieb**	**12**
5.1	Vnútorná organizácia	12
5.1.1	Spoľahlivosť organizácie	12
5.1.2	Delenie povinností	12
5.2	Ľudské zdroje	12
5.3	Správa aktív	14
5.3.1	Všeobecné požiadavky	14
5.3.2	Manipulácia s médiami	14
5.4	Riadenie prístupu	14
5.5	Kryptografické riadiace prvky	15
5.6	Fyzická a objektová bezpečnosť	15
5.7	Prevádzková bezpečnosť	15
5.8	Sieťová bezpečnosť	16
5.9	Riadenie bezpečnostných incidentov	17
5.10	Zber dôkazov	18
5.11	Riadenie kontinuity činnosti organizácie	18
5.12	Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti	19
5.13	Zhoda	19
5.14	Orgán dohľadu	20

1 Úvod

Tento dokument špecifikuje politiku Národnej agentúry pre sieťové a elektronické služby so sídlom Kollárova 8, 917 02 Trnava, Detašované pracovisko: BC Omnipolis, Trnavská cesta 100/II, 821 01 Bratislava, IČO: 42 156 424 (ďalej len „NASES“) ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“).

Politika poskytovania dôveryhodných služieb platí pre všetky dôveryhodné služby (uvedené v kapitole 2), poskytované Poskytovateľom. NASES uvedené služby poskytuje prostredníctvom certifikačnej autority SNCA, ktorá je prevádzkovaná v systéme IS KDS.

Táto politika:

- vychádza z požiadaviek legislatívnych a normatívnych dokumentov, uvedených v kapitole 1, najmä však v dokumente ETSI EN 319 401 1;
- má všeobecný charakter a nemusí definovať všetky špecifické požiadavky, kladené na jednotlivé poskytované dôveryhodné služby;
- nešpecifikuje, ako majú byť jednotlivé požiadavky na poskytovateľa dôveryhodných služieb posudzované nezávislými tretími stranami, vrátane požiadaviek na informácie, ktoré majú byť k dispozícii nezávislým posudzovateľom, alebo požiadavky na takýchto posudzovateľov.

1.1 Identifikácia dokumentu

Tomuto dokumentu je priradený identifikátor objektu (OID):

1.3.158.42156424.0.1.1

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovensko (Slovakia)
42156424	jedinečný identifikátor Národnej agentúry pre sieťové a elektronické služby priradený organizáciou ISO (IČO)
0	KCA (poskytovanie dôveryhodných služieb)
1	Certifikačné politiky
1	Politika poskytovania dôveryhodných služieb NASES

2 Všeobecné ustanovenia

Dôveryhodné služby v zmysle certifikačnej schémy orgánu dohľadu [5], na ktoré sa vzťahuje táto politika sú:

- Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis.
- Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre elektronickú pečať.
- Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov pre autentifikáciu webových sídiel.
- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov.
- Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí.
- Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov.
- Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických pečatí.
- Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok.

3 Posúdenie rizík

Poskytovateľ vykonáva posúdenie rizík s cieľom identifikovať, analyzovať a vyhodnocovať riziká, súvisiace s poskytovaním dôveryhodnej služby, s ohľadom na obchodné a technické otázky. Posúdenie sa vykonáva podľa metodiky uvedenej v Štandarde RM 1.

Poskytovateľ vyberá vhodné opatrenia na riadenie rizík na základe výsledkov posúdenia rizík, pričom tieto opatrenia musia garantovať, aby úroveň zabezpečenia bola primeraná a úmerná stupňu rizika.

Poskytovateľ určuje všetky bezpečnostné požiadavky a prevádzkové postupy, ktoré sú nevyhnutné pre implementáciu opatrení na riadenie rizík.

Opatrenia na riadenie rizík sú zdokumentované v tejto politike a nadväzných dokumentoch informačnej bezpečnosti a v pravidlách na vykonávanie dôveryhodných služieb.

Posúdenie rizík je pravidelne revidované.

Vedenie Poskytovateľa, v procese riadenia rizík, schvaľuje výsledky posúdenia rizík a akceptuje zvyškové riziká.

4 Politiky a praktiky

4.1 Politiky a pravidlá pre poskytovanie dôveryhodných služieb

Poskytovateľ špecifikuje množinu politík a pravidiel pre poskytované dôveryhodné služby. Tieto politiky a pravidlá sú schválené Poskytovateľom a publikované na úložisku Poskytovateľa, resp. komunikované pracovníkom Poskytovateľa a relevantným externým stranám.

Všeobecné povinnosti Poskytovateľa:

- Poskytovateľ musí mať stanovené pravidlá a postupy, ktoré pokryjú požiadavky, identifikované v politikách Poskytovateľa.
- Poskytovateľ musí mať pravidlá, identifikujúce záväzky všetkých externých organizácií, podporujúcich poskytovanie dôveryhodných služieb Poskytovateľa, vrátane aplikovateľných politík a postupov.
- Pravidlá a postupy Poskytovateľa, musia byť dostupné Odberateľom a Spoliehajúcim sa stranám spoločne s ďalšou relevantnou dokumentáciou (ak je to nutné k posúdeniu zhody s politikou služby).
- Poskytovateľ má celkovú zodpovednosť za poskytovanie dôveryhodných služieb a konečnú právomoc na schvaľovanie politík a postupov.
- Poskytovateľ musí zabezpečiť, aby vedenie Prevádzkovateľa disponovalo takými právomocami, ktoré mu umožňujú zabezpečiť implementáciu politík a pravidiel a poskytovať dostatočnú podporu pre poskytovanie dôveryhodných služieb.
- Poskytovateľ musí mať definovaný proces aktualizácie politík a pravidiel, vrátane zodpovedností za udržiavanie týchto politík a pravidiel.
- Poskytovateľ musí mať definovaný postup upozorňovania na zamýšľané zmeny v politikách a pravidlách a po ich schválení, postupy na ich sprístupnenie.
- Poskytovateľ musí mať definované politiky a pravidlá pre prípad ukončenia poskytovania dôveryhodnej služby.

4.2 Všeobecné podmienky

Všeobecné podmienky, týkajúce sa služieb Poskytovateľa, sú sprístupnené všetkým Odberateľom a Spoliehajúcim sa stranám. Tieto všeobecné podmienky, špecifikujú pre politiku každej dôveryhodnej služby, podporovanej Poskytovateľom, minimálne:

- aplikovanú politiku dôveryhodnej služby,
- každé obmedzenie pri použití služby (napr. doba platnosti certifikátu),
- povinnosti Odberateľa, ak existujú,
- informácie pre Spoliehajúce sa strany (napr. spôsob, ako verifikovať token dôveryhodnej služby),

- časové obdobie, počas ktorého Poskytovateľ uchováva záznamy o udalostiach,
- obmedzenia zodpovednosti,
- obmedzenia pri použití poskytovanej služby, vrátane obmedzenia práva na náhradu škody, vzniknutej pri použití služby spôsobom, prekračujúcim tieto obmedzenia,
- aplikovateľnú legislatívu,
- postupy pre vybavenie sťažností a urovnávanie sporov,
- informáciu, či dôveryhodná služba Poskytovateľa bola posúdená s ohľadom na súlad s politikou dôveryhodných služieb, a ak áno, prostredníctvom akej schémy posudzovania,
- kontaktné údaje Poskytovateľa.

Odberatelia a Spoliehajúce sa strany sú informovaní o všeobecných podmienkach pred uzatvorením zmluvného vzťahu s Poskytovateľom. Všeobecné podmienky sú Odberateľom a Spoliehajúcim sa stranám dostupné prostredníctvom trvalých komunikačných prostriedkov v čitateľnom a zrozumiteľnom jazyku. Všeobecné podmienky môžu byť šírené elektronicky.

4.3 Politika informačnej bezpečnosti

Poskytovateľ má definovanú politiku informačnej bezpečnosti, ktorá stanovuje jeho prístup k riadeniu informačnej bezpečnosti a ktorá je schválená vedením Poskytovateľa.

Zmeny, vykonané v politike informačnej bezpečnosti, sú v prípade potreby oznámené tretím stranám, ktorými sú Odberatelia, Spoliehajúce sa strany, dodávatelia, hodnotiace, dozorné a iné regulačné orgány.

Povinnosti Poskytovateľa vo vzťahu k informačnej bezpečnosti:

- Poskytovateľ musí mať zdokumentovanú, implementovanú a udržiavanú politiku informačnej bezpečnosti, vrátane riadenia bezpečnostných kontrol a prevádzkových postupov pre zariadenia, systémy a informačné prostriedky SNCA.
- Poskytovateľ musí sprístupniť a komunikovať politiku informačnej bezpečnosti všetkým pracovníkom Poskytovateľa, ktorých sa táto politika týka.
- Poskytovateľ preberá plnú zodpovednosť za súlad s postupmi, predpísanými v politike informačnej bezpečnosti a to aj vtedy, ak funkcionalita SNCA je zabezpečená inými dodávateľmi. Poskytovateľ musí mať definované záväzky dodávateľov a zabezpečiť, aby bol dodávateľ viazaný povinnosťou implementovať akékoľvek kontroly, požadované Poskytovateľom.
- Politika informačnej bezpečnosti a zoznam aktív Poskytovateľa, musia byť revidované v plánovaných intervaloch alebo v prípade vzniku významných zmien, s cieľom zabezpečiť ich trvalú vhodnosť, primeranosť a účinnosť. Konfigurácia komponentov IS KDS musí byť pravidelne kontrolovaná na zmeny, ktoré môžu porušovať bezpečnostné politiky Poskytovateľa.

5 Riadenie a prevádzka dôveryhodných služieb

5.1 Vnútorná organizácia

5.1.1 Spoľahlivosť organizácie

Poskytovateľ sa považuje za spoľahlivú organizáciu, pretože:

- Politiky a pravidlá dôveryhodnej služby, na základe ktorých Poskytovateľ pôsobí, sú nediskriminačné.
- Služby Poskytovateľa sú prístupné všetkým Odberateľom, ktorý svojou podstatou spadajú do oblasti pôsobnosti Poskytovateľa a ktorí súhlasia s tým, že budú dodržiavať svoje povinnosti, uvedené vo všeobecných a zmluvných podmienkach Poskytovateľa.
- Poskytovateľ, v súlade s vnútroštátnymi právnymi predpismi, disponuje dostatočnými finančnými zdrojmi a/alebo primeraným poistením zodpovednosti za škodu pre potreby krytia záväzkov, vyplývajúcich z činnosti a aktivít Poskytovateľa.
- Poskytovateľ disponuje dostatočnými finančnými a inými zdrojmi, potrebnými na prevádzku dôveryhodných služieb, v súlade s touto politikou.
- Poskytovateľ má politiky a postupy na riešenie sťažností a sporov, prijatých od Odberateľov alebo Spoliehajúcich sa strán, týkajúcich sa poskytovania služieb a/alebo iných súvisiacich záležitostí.
- Poskytovateľ má zdokumentovanú dohodu a zmluvný vzťah, ak poskytovanie služieb zahŕňa subdodávateľské zmluvy, outsourcing alebo iné dohody s tretími stranami.

5.1.2 Delenie povinností

Povinnosti alebo oblasti zodpovednosti a oprávnenia, ktoré môžu byť v konflikte sú oddelené, aby sa redukovali riziká, súvisiace s nepovolenou alebo neúmyselnou zmenou alebo zneužitím aktív Poskytovateľa.

5.2 Ľudské zdroje

Poskytovateľ zabezpečuje, že pracovníci Poskytovateľa a zmluvní pracovníci Poskytovateľa, podporujú dôveryhodnosť služieb SNCA a to nasledovne:

- Poskytovateľ zamestnáva pracovníkov, ktorí disponujú potrebnými odbornými znalosťami, sú spoľahliví, majú dostatočné skúsenosti a absolvovali školenia, týkajúce sa pravidiel bezpečnosti a ochrany osobných údajov, ktoré sú vhodné pre ponúkané služby a pracovnú pozíciu, resp. pracovnú náplň pracovníka Poskytovateľa.

- Pracovníci Poskytovateľa sú schopní spĺňať požiadavky „odborných vedomostí, skúseností a kvalifikácie“ prostredníctvom formálneho vzdelávania, školení a certifikátov, prípadne prostredníctvom reálnych skúseností alebo kombináciou oboch.
- V prípade porušenia politík a postupov Poskytovateľa jeho pracovníkmi, budú voči pracovníkom, ktorí porušenie zapríčinili, uplatňované primerané disciplinárne sankcie.
- Bezpečnostné role a k nim prináležiace zodpovednosti (špecifikované v politike informačnej bezpečnosti Poskytovateľa), sú zdokumentované v popise práce alebo v dokumentoch, dostupných všetkým zainteresovaným pracovníkom. Dôverné role, na ktorých závisí bezpečnosť prevádzky SNCA, sú jasne identifikované. Tieto role sú menované a akceptované vedením Poskytovateľa a osobou, ktorá v danej roli pracuje.
- Zamestnanci Poskytovateľa (dočasní aj trvalí) majú definovaný popis práce z pohľadu rolí. Popis práce zohľadňuje delenie oprávnení a zodpovedností, minimálnych nárokov (odstavec 7.1.2), určuje citlivosť pracovnej pozície, založenej na povinnostiach a úrovni prístupu, potrebné školenia a uvedomenie si ich zodpovednosti. Poskytovateľ, tam kde je to vhodné, rozlišuje medzi všeobecnými funkciami a špecifickými funkciami.
- Pracovníci Poskytovateľa používajú administratívne a riadiace postupy, ktoré sú v súlade s politikami riadenia informačnej bezpečnosti Poskytovateľa.
- Riadiaci pracovníci Poskytovateľa majú skúsenosti alebo odbornú prípravu, resp. školenia v súvislosti s poskytovanou dôveryhodnou službou. Riadiaci pracovníci sú oboznámení s bezpečnostnými postupmi, určenými pre pracovníkov v dôveryhodných roliach, majú dostatočné bezpečnostné povedomie a skúsenosti s povinnosťami v oblasti riadenia informačnej bezpečnosti a posudzovania rizík. Tieto skúsenosti sú dostatočné pre vykonávanie riadiacej funkcie Poskytovateľa.
- Pracovníci Poskytovateľa, pracujúci v dôverných rolách, sa nenachádzajú v konflikte záujmov, ktorý by mohol ovplyvniť zainteresovanosť pracovníka na spoľahlivej prevádzke dôveryhodných služieb Poskytovateľa.
- Dôveryhodné role zahŕňajú nasledovné zodpovednosti:
  - Bezpečnostný manažér – má celkovú zodpovednosť za správu a implementáciu bezpečnostných postupov v oblasti ochrany informácií a aktív Poskytovateľa.
  - PMA - vrcholová autorita pre riadenie politík systému dôveryhodných služieb.
  - Administrátor dôveryhodných služieb – inštaluje, konfiguruje a udržiava dôveryhodný systém Poskytovateľa z pohľadu poskytovania dôveryhodných služieb.
  - Bezpečnostný správca – má zodpovednosť za bezpečnosť prevádzky systému dôveryhodných služieb.
  - Systémový administrátor – má zodpovednosť za inštaláciu, konfiguráciu, každodennú prevádzku a zálohovanie komponentov dôveryhodného systému Poskytovateľa.

- Operátor RA - zabezpečuje registračné procesy, odovzdávanie a zrušovanie certifikátov vydaných Držiteľom
- Interný audítor – je autorizovaný na prezeranie archívov a auditných záznamov dôveryhodného systému Poskytovateľa.

- Pracovníci Poskytovateľa sú do dôveryhodných rolí formálne menovaní riadiacim pracovníkom Poskytovateľa.
- Pracovníci Poskytovateľa majú prístup k dôveryhodným funkciám až po vykonaní všetkých požadovaných a nevyhnutých kontrol.

5.3 Správa aktív

5.3.1 Všeobecné požiadavky

Poskytovateľ musí prostredníctvom implementovaných opatrení zabezpečiť vhodnú úroveň ochrany svojich aktív (vrátane informačných aktív dôveryhodného systému).

Poskytovateľ musí udržiavať aktuálny zoznam svojich informačných aktív a jednoznačne prideľovať zodpovednosti za ich ochranu.

Jednotlivé aktíva musia byť klasifikované v súlade s úrovňou súvisiacich rizík.

5.3.2 Manipulácia s médiami

S každým médiom musí byť zaobchádzané bezpečne, v zmysle požiadaviek klasifikačnej schémy.

Médiá, obsahujúce citlivé údaje, musia byť bezpečne zlikvidované, ak už nie sú ďalej potrebné.

5.4 Riadenie prístupu

Prístup do dôveryhodného systému musí byť povolený len pre autorizovaných jednotlivcov a je riadený nasledovne:

- Prvky ochrany (napr. firewall) chránia internú PKI infraštruktúru Poskytovateľa pred neoprávneným prístupom, vrátane prístupu Odberateľov a tretích strán. Firewally sú nakonfigurované v záujme prevencie tak, že povoľujú len protokoly a prístupy nevyhnutné pre prevádzku SNCA.
- Prístupy operátorov, administrátorov a audítorov systému, sú pod kontrolou Poskytovateľa. To zahŕňa správu používateľských účtov a včasnú aktualizáciu alebo odstránenie prístupov.
- Prístup k informáciám a funkciám systému je obmedzený v zmysle politiky riadenia prístupu. Systém Poskytovateľa poskytuje vhodné prvky počítačovej bezpečnosti

na oddelenie dôveryhodných rolí, identifikovaných v postupoch Poskytovateľa. Oddelenie dôveryhodných rolí zahŕňa aj oddelenie funkcií riadenia bezpečnosti a prevádzky.

- Pracovníci Poskytovateľa sú identifikovaní a autorizovaní pred použitím kritických aplikácii, ktoré súvisia s dôveryhodnými službami.
- Aktivity pracovníkov Poskytovateľa sú v rámci SNCA zaznamenávané.
- Ochrana citlivých údajov je zaisťovaná aj voči obnoveniu údajov neoprávneným používateľom v prípade opätovného použitia pamäťových objektov (napr. odstránených súborov).

5.5 Kryptografické riadiace prvky

Na správu všetkých kryptografických kľúčov a zariadení sú počas ich životného cyklu použité primerané bezpečnostné prvky a opatrenia.

5.6 Fyzická a objektová bezpečnosť

Poskytovateľ má v oblasti fyzickej a objektovej bezpečnosti prijaté opatrenia, zabraňujúce strate, poškodeniu, kompromitovaniu alebo odcudzeniu informácií a prostriedkov spracovania informácií a tým prerušeniu poskytovania dôveryhodných služieb:

- Poskytovateľ riadi fyzický prístup ku komponentom IS KDS, ktorých bezpečnosť je kritická pre poskytovanie dôveryhodných služieb - prístup je umožnený len oprávneným jednotlivcom.
- Komponenty, kritické z pohľadu zabezpečenia prevádzky dôveryhodných služieb, sú umiestnené v chránených bezpečných priestoroch, ktoré disponujú fyzickou ochranou proti vniknutiu. Bezpečné priestory majú implementované opatrenia pre zabezpečenie kontroly prístupu a signalizáciu pre prípad detegovania nežiaduceho vstupu do priestorov.

5.7 Prevádzková bezpečnosť

Poskytovateľ používa dôveryhodný systém a produkty, ktoré sú chránené voči zmenám a ktoré zabezpečujú technickú bezpečnosť a spoľahlivosť nimi podporovaných procesov, konkrétne:

- Pre nasadzovanie, zmenu, núdzové opravy alebo aktualizáciu konfigurácií akéhokoľvek systému Poskytovateľa, na ktorý sa aplikuje bezpečnostná politika, sú použité postupy riadenia zmien. Tieto postupy zahŕňajú dokumentáciu realizovaných zmien a posúdenie dopadu zmien na bezpečnosť systému.
- Úplnosť (integrita) informácii a systémov Poskytovateľa je chránená proti škodlivému kódu a neoprávnenému prístupu.

- S médiami, používanými v systémoch Poskytovateľa, je zaobchádzané bezpečne, aby nedošlo k ich poškodeniu, odcudzeniu alebo neoprávnenému prístupu.
- Poskytovateľ má určený životný cyklus médií, ktorý sleduje zastaranosť médií počas doby ich používania a uchovávania.
- Poskytovateľ má stanovené a implementované postupy pre všetky dôveryhodné a administratívne roly, ktoré sa podieľajú na poskytovaní služieb.
- Poskytovateľ má špecifikované a aplikované postupy pre zabezpečenie:
  - aplikovania bezpečnostných záplat v primeranom čase od kedy sú dostupné.
  - neaplikovania bezpečnostných záplat, ktoré predstavujú ďalšiu zraniteľnosť alebo nestabilitu systému, ktoré prevažujú nad výhodami ich aplikovania. Dôvody neaplikovania bezpečnostnej záplaty sú zdokumentované.

5.8 Sieťová bezpečnosť

Poskytovateľ chráni svoju infraštruktúru a systémy dôveryhodných služieb pred útokom, najmä:

- rozdelením systémov do sietí a zón, založených na posúdení rizík, s ohľadom na funkčné, logické a fyzické vzťahy medzi systémami a službami. Poskytovateľ aplikuje rovnaké bezpečnostné opatrenia na všetky systémy umiestnené v tej istej zóne.
- obmedzením prístupov a komunikácie medzi zónami len na nevyhnutné prípady z pohľadu zabezpečenia prevádzky systému Poskytovateľa. Nepotrebné prepojenia a služby sú zakázané alebo deaktivované a zavedený súbor pravidiel je pravidelne posudzovaný.
- udržiavaním systémov, ktoré sú z pohľadu prevádzky Poskytovateľa kritické, vo vyhradených bezpečných zónach.
- oddelením sietí, dedikovaných pre správu IT systémov, od ostatných prevádzkových sietí Poskytovateľa.
- oddelením produkčného systému dôveryhodných služieb Poskytovateľa od systému používaného na vývoj a testovanie.
- zabezpečením komunikácie medzi rozdielnymi dôveryhodnými systémami prostredníctvom dôveryhodných kanálov, ktoré sú logicky odlíšené od ostatných komunikačných kanálov a poskytujú zabezpečenú identifikáciu svojich koncových bodov a ochranu dátových kanálov pred zmenou a prezradením.
- zabezpečením vysokej úrovne dostupnosti dôveryhodných služieb a to pomocou redundantného prístupu do siete, ktorý zabezpečí dostupnosť služby aj pri vzniku jednoduchej chyby.
- vykonávaním pravidelného vyhľadávania zraniteľnosti na verejných aj interných IP adresách, ktoré Poskytovateľ používa a vytváraním evidencie, ktorá dokazuje, že každé takéto vyhľadávanie bolo vykonané osobou alebo subjektom, ktorý má

potrebné a požadované zručnosti, boli použité vhodné nástroje, bol dodržaný etický kódex a nezávislosť, nevyhnutná na poskytnutie hodnovernej správy.

- vykonávaním penetračných testov na systémoch Poskytovateľa po zriadení, aktualizácii alebo zmene, ktoré Poskytovateľ identifikuje ako podstatné. Poskytovateľ eviduje záznam o každom vykonanom penetračnom teste v rozsahu:
  - či bol realizovaný osobou alebo subjektom, ktorý má potrebné a požadované zručnosti,
  - či boli použité vhodné nástroje,
  - či bol dodržaný etický kódex a nezávislosť, ktorá je nevyhnutná na poskytnutie hodnovernej správy.

5.9 Riadenie bezpečnostných incidentov

Aktivity, týkajúce sa prístupov a využívania informačných systémov Poskytovateľa, ako aj požiadavky na služby, sú na úrovni systémov monitorované, pričom:

- Úroveň a detailnosť monitorovania závisí od charakteru a kritickosti monitorovaných informačných aktív.
- Abnormálne systémové aktivity, ktoré naznačujú potenciálne porušenie bezpečnosti (napr. vniknutie do siete Prevádzkovateľa), sú detegované a hlásené ako výstraha.
- IT systémy Poskytovateľa monitorujú minimálne nasledovné udalosti:
  - spustenie a vypnutie logovacích funkcionalít,
  - dostupnosť a využitie služieb v sieti Poskytovateľa.
- V prípade vzniku incidentu Poskytovateľ koná včas a koordinovane s cieľom obmedziť dosah porušenia bezpečnosti. Poskytovateľ má menovaných pracovníkov v dôveryhodných roliach, ktorí sledujú výstrahy možných kritických bezpečnostných udalostí a zabezpečujú, aby boli príslušné incidenty hlásené v súlade s postupmi Poskytovateľa.
- Poskytovateľ má v súlade s platnými regulačnými pravidlami zavedené postupy pre informovanie príslušných strán o každom porušení bezpečnosti (strate dôvernosti, dostupnosti alebo integrity), ktorá má významný dopad na poskytované dôveryhodné služby a spracúvané osobné údaje, a to do 24 hodín od identifikácie porušenia.
- Ak porušenie bezpečnosti môže nepriaznivo ovplyvniť fyzickú alebo právnickú osobu, ktorej bola poskytnutá dôveryhodná služba, Poskytovateľ bezodkladne o tejto skutočnosti informuje dotknutú osobu.
- Poskytovateľ pravidelne posudzuje auditné záznamy s cieľom identifikovať dôkazy o škodlivých aktivitách a to implementovaním automatických mechanizmov na spracovanie auditných záznamov a informovanie personálu na možné kritické bezpečnostné udalosti.

- Poskytovateľ rieši každú kritickú zraniteľnosť do 48 hodín od identifikovania tejto zraniteľnosti. Ak je to nákladovo efektívne, Poskytovateľ naplánuje a implementuje opatrenia na zmiernenie zraniteľnosti. V prípade, že zraniteľnosť nie je z jej povahy a závažnosti potrebné odstrániť, je takéto rozhodnutie zdôvodnené a zdokumentované.
- Postupy, hlásenia a reakčné postupy, sú používané takým spôsobom, aby sa minimalizovali škody spôsobené bezpečnostnými incidentmi a poruchami.

5.10 Zber dôkazov

Poskytovateľ zaznamenáva a v primeranej dobe udržuje dostupné všetky relevantné informácie, týkajúce sa vydaných a prijatých údajov a to aj v prípade, že Poskytovateľ už neposkytuje dôveryhodné služby. Tieto úkony musí Poskytovateľ vykonávať pre prípad potreby poskytnutia dôkazov v súdnom konaní a zabezpečenia kontinuity služieb.

Poskytovateľ spomenuté docieli:

- udržiavaním dôvernosti a integrity auditných záznamov, týkajúcich sa prevádzky dôveryhodných služieb.
- bezpečným archivovaním záznamov, týkajúcich sa prevádzky služieb. Archivácia záznamov je realizovaná v súlade so zverejnenými obchodnými praktikami.
- sprístupnením auditných záznamov, týkajúcich sa dôverných služieb na účely poskytnutia dôkazu o správnom fungovaní služieb v prípade súdneho konania.
- zaznamenávaním presného času auditovaných udalostí v prostredí Poskytovateľa, správy kľúčov a synchronizácie hodín, pričom tento čas musí byť minimálne raz denne synchronizovaný s UTC.
- uchovávaním auditných záznamov, týkajúcich sa služieb po dobu, ktorá je potrebná na poskytnutie potrebných právnych dôkazov a ktorá je oznámená v podmienkach Poskytovateľa.
- zaznamenávaním udalostí tak, aby auditné záznamy nebolo možné jednoducho odstrániť alebo zničiť (s výnimkou prípadu, keď sú predtým spoľahlivo prenesené na archivačné média) a to v čase, keď sa vyžaduje ich uchovávanie.

5.11 Riadenie kontinuity činnosti organizácie

Poskytovateľ má definovaný a udržiavaný plán kontinuity činností, ktorý je aktivovaný v prípade vzniku katastrofy. V prípade katastrofy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých údajov Poskytovateľa), musí byť prevádzka SNCA obnovená v rámci oneskorenia definovaného v pláne kontinuity činností.

5.12 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Poskytovateľ má vypracovaný a prijatý plán ukončenia poskytovania služieb. Pred ukončením poskytovania svojich služieb, aplikuje minimálne nasledovné postupy:

- O ukončení poskytovania služieb informuje všetkých Odberateľov a iné entity, s ktorými má Poskytovateľ uzatvorené zmluvy alebo iné formy vzťahov. O ukončení poskytovania služieb informuje aj Spoliehajúce sa strany.
- Ukončí autorizáciu všetkých subdodávateľov, ktorí konali v zastúpení Poskytovateľa pri vykonávaní akýchkoľvek funkcií súvisiacich s procesom vydávania tokenov pre dôveryhodné služby.
- Prenesie všetky záväzky, týkajúce sa uchovávania informácií, potrebných na poskytovanie dôkazov o prevádzke dôveryhodných služieb, počas primerane stanovenej doby na spoľahlivú stranu (v zmysle § 4, odsek (2) Zákona o DS).
- Zničí (vrátane kópií) alebo stiahne z používania primárne kľúče takým spôsobom, že ich nebude možné znovu obnoviť a používať.
- Vytvorí dohodu (ak je to možné) o prevode poskytovania dôveryhodných služieb pre svojich súčasných Odberateľov na iného poskytovateľa dôveryhodných služieb (v zmysle § 4, odsek (2) Zákona o DS).

Poskytovateľ má prijatú dohodu o krytí nákladov na splnenie týchto minimálnych požiadaviek v prípade, že Poskytovateľ zanikne alebo z iných dôvodov nie je schopný pokryť náklady sám, a to s ohľadom na platnú legislatívu.

Poskytovateľ bude dodržiavať svoje záväzky o sprístupnení svojho verejného kľúča alebo dôkazov o poskytovaných dôveryhodných službách Spoliehajúcim sa stranám počas primeranej doby, resp. prevedie tieto záväzky na inú dôveryhodnú osobu.

5.13 Zhoda

Poskytovateľ svoje dôveryhodné služby poskytuje v súlade s platnou legislatívou a takým spôsobom aby:

- disponoval dôkazmi, že spĺňa legislatívne požiadavky súvisiace s poskytovaním dôveryhodných služieb (§ 5 Zákona o DS),
- mohli byť dôveryhodné služby Poskytovateľa a s nimi súvisiace produkty poskytnuté aj osobám s telesným postihnutím,
- prijaté technické a organizačné opatrenia boli primerané a účinné proti neoprávnenému spracovaniu osobných údajov a proti náhodnej strate, zničeniu alebo poškodeniu osobných údajov.

5.14 Orgán dohľadu

Poskytovateľ je povinný pri komunikácii s orgánom dohľadu v zmysle požiadaviek Nariadenia eIDAS 1 a Zákona o DS 1:

- ak zamýšľa začať poskytovať kvalifikované dôveryhodné služby, predložiť orgánu dohľadu oznámenie o svojom zámere spolu so správou o posúdení zhody, ktorú vydal orgán posudzovania zhody,
- poskytnúť úradu informácie o zmenách v jeho kvalifikovaných dôveryhodných službách najneskôr do 30 dní pred plánovanou zmenou,
- zasielať orgánu dohľadu:
  - vydané kvalifikované certifikáty pre kvalifikovaný elektronický podpis a pre kvalifikovanú elektronickú pečať do 30 dní od ich vydania,
  - potvrdenie o dátume a čase zrušenia kvalifikovaných certifikátov do 30 dní od ich zrušenia,
  - 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,
- oznámiť orgánu dohľadu bez zbytočného odkladu, najneskôr však do 24 hodín, odkedy sa dozvedel o akomkoľvek narušení bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje, uchovávané v rámci nej.

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