Národná agentúra pre sieťové a elektronické služby

Politika poskytovania dôveryhodných služieb

Verzia dokumentu	1.0
Dátum vydania	27.07.2017
Názov dokumentu	Politika poskytovania dôveryhodných služieb
Gestor	Sekcia bezpečnosti
Vlastník	NASES

OBSAH:

1. ÚVOD

Tento dokument špecifikuje politiku Národnej agentúry pre sieťové a elektronické služby, so sídlom Kollárova 8, 917 02 Trnava (ďalej aj „NASES“), ktorá vychádza z požiadaviek uvedených v dokumente ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers" [1] a má slúžiť ako potvrdenie úrovne bezpečnosti poskytovaných služieb, ktoré spočívajú v generovaní a spravovaní údajov na vyhotovenie kvalifikovanej elektronickej pečate pre potreby tretích strán (ďalej len „dôveryhodná služba“), tak ako je to uvedené v bode 51 preambuly Nariadenia 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 len „Nariadenie eIDAS“). Táto politika NASES (ďalej len „Poskytovateľ“):

a) definuje požiadavky, ktorých naplnenie je nevyhnutné uplatňovať v rámci riadenia a prevádzky poskytovania služieb Poskytovateľa pre tretie strany,
b) má všeobecný charakter a nemusí pokrývať všetky špecifické požiadavky kladené na poskytované dôveryhodné služby.
c) nešpecifikuje ako majú byť jednotlivé požiadavky na Poskytovateľa posudzované nezávislými tretími stranami, vrátane požiadaviek na informácie, ktoré majú byť k dispozícii nezávislým posudzovateľom, alebo požiadavky na takýchto posudzovateľov.

1.1. Identifikácia CP

Tejto politike bol pridelený OID v tvare:

1.3.158. 42156424.0.0.1.0.1

kde jednotlivé zložky OID majú nasledovný význam:

1.	ISO
1.3.	Identified Organization
1.3.158.	IČO
1.3.158.42156424.	NASES
1.3.158. 42156424.0.	Vyhradené pre NASES
1.3.158. 42156424.0.0.	Vyhradené pre NASES
1.3.158. 42156424.0.0.1.	Služba správy zverených údajov na vyhotovenie kvalifikovanej elektronickej pečate do starostlivosti tretej strany
1.3.158. 42156424.0.0.1.0	Vyhradené pre NASES
1.3.158. 42156424. 0.0.1.0.1	CP TSP

1.2. Správa politiky

Za obsah tejto politiky zodpovedá:

Národná agentúra pre sieťové a elektronické služby
Kollárova 8, 917 02 Trnava
IČO 42156424
Detašované pracovisko:
BC Omnipolis, Trnavská cesta 100/II, 821 01 Bratislava
Tel.: +421 2 3278 0700
e-mail: info@nases.gov.sk

2. ODKAZY NA ŠTANDARDY A LEGISLATÍVU

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

[2] Nariadenia 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
[3] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management"
[4] STN P CEN/TS 419241:2014: Bezpečnostné požiadavky na dôveryhodné systémy podporujúce serverové podpisovanie
[5] NBÚ - Certifikačná schéma pre eIDAS, Verzia 0.3

3. POJMY A SKRATKY

3.1. Pojmy

Použité pojmy sú prevzaté z Nariadenia EPaR (EÚ) č. 910/2014 [2] (ďalej len „Nariadenia eIDAS“) a normy ETSI EN 319 401 [1].

Spoliehajúca sa strana	Fyzická alebo právnická osoba spoliehajúca sa na elektronickú identifikáciu alebo dôveryhodnú službu.
Odberateľ	
Orgán dohľadu	Orgán usadený na území členského štátu, ktorý je zodpovedný za úlohy dohľadu v určujúcom členskom štáte.
Orgán posudzovania zhody	Orgán vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008, ktorý je v súlade s uvedeným nariadením akreditovaný ako orgán príslušný na posudzovanie zhody kvalifikovaných poskytovateľov dôveryhodných služieb a kvalifikovaných dôveryhodných služieb, ktoré poskytujú.
Politika dôveryhodnej služby	Súbor pravidiel, ktoré indikujú použiteľnosť dôveryhodnej služby pre konkrétnu komunitu a/alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami.
Poskytovateľ dôveryhodných služieb	Fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb

3.2. Skratky

CA	Certifikačná autorita (Certification Authority)
TSP	Poskytovateľ dôveryhodných služieb (Trust Service Provider)

4. VŠEOBECNÉ USTANOVENIA

Aj keď v súčasnosti v dokumente „Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu“ vo verzii 1.3 z 3.3.2017 nie je národným orgánom dohľadu pre oblasť Nariadenia eIDAS, ktorým je Národný bezpečnostný úrad, definovaná služba správy zverených údajov na vyhotovenie kvalifikovanej elektronickej pečate do starostlivosti tretej strany, rozhodol sa Poskytovateľ preukázať touto politikou, že ním poskytovaná služba správy takýchto údajov je plne konformná s požiadavkami, ktoré sú kladené na poskytovateľov obdobných služieb definovaných v Nariadení eIDAS, čím chce preukázať tretím stranám, ktorým údaje spravuje ako aj Spoliehajúcim sa stranám splnenie požiadavky uvedenej v bode 3 Prílohy č. II Nariadenia eIDAS.

5. POSÚDENIE RIZÍK

Poskytovateľ musí vykonať posúdenie rizík s cieľom identifikovať, analyzovať a vyhodnotiť riziká súvisiace s poskytovaním dôveryhodnej služby s ohľadom na obchodné a technické otázky. Poskytovateľ musí vybrať vhodné opatrenia na riadenie rizík, pričom zohľadní výsledky posúdenia rizík. Opatrenia na riadenie rizík musia zabezpečiť, že úroveň zabezpečenia je primeraná a úmerná stupňu rizika.

Poskytovateľ musí určiť všetky bezpečnostné požiadavky a prevádzkové postupy, ktoré sú nevyhnutné pre implementáciu opatrení na riadenie rizík. Opatrenia na riadenie rizík musia byť zdokumentované v politike informačnej bezpečnosti a v pravidlách na vykonávanie dôveryhodných služieb.
Posúdenie rizík musí byť pravidelne posudzované a revidované.
Manažment Poskytovateľa musí schváliť posúdenie rizík a akceptované zvyškové riziká.

6. POLITIKY A PRAKTIKY

6.1. Politiky a pravidlá pre poskytovanie dôveryhodných služieb

Poskytovateľ musí špecifikovať množinu politík a pravidiel pre poskytované dôveryhodné služby. Tieto politiky a pravidlá musia byť schválené manažmentom a publikované, resp. komunikované zamestnancom a relevantným externým stranám.
Povinnosti poskytovateľa:

a) Poskytovateľ musí mať pravidlá a postupy, ktoré pokryjú požiadavky identifikované aplikovateľnou politikou Poskytovateľa.
b) Poskytovateľ musí mať pravidlá identifikujúce záväzky všetkých externých organizácií podporujúcich dôveryhodné služby Poskytovateľa, vrátané aplikovateľných politík a postupov.
c) Pravidlá a postupy Poskytovateľa musia byť dostupné Odberateľom a Spoliehajúcim sa stranám spolu s ďalšou relevantnou dokumentáciou (ak je to nutné k posúdeniu zhody s politikou služby).
d) Poskytovateľ musí mať riadiaci orgán s celkovou zodpovednosťou za Poskytovateľa s konečnou právomocou na schvaľovanie politík a postupov Poskytovateľa.
e) Poskytovateľ musí mať určený manažment, ktorý zabezpečí implementáciu politík a pravidiel.
f) Poskytovateľ musí mať definovaný proces aktualizácie politík a pravidiel, vrátane zodpovedností za udržiavanie týchto politík a pravidiel.
g) Poskytovateľ musí mať definovaný postup upozorňovania na zamýšľané zmeny v politikách a pravidlách a po ich schválení postupy na ich sprístupnenie.
h) Poskytovateľ musí mať definované politiky a pravidlá pre prípad ukončenia poskytovania dôveryhodnej služby.

6.2. Všeobecné podmienky

Všeobecné podmienky týkajúce sa služieb Poskytovateľa budú sprístupnené všetkým Odberateľom a Spoliehajúcim sa stranám len na požiadanie.
Tieto všeobecné podmienky musia špecifikovať pre politiku každej dôveryhodnej služby podporovanej Poskytovateľom minimálne:

a) aplikovanú politiku dôveryhodnej služby,
b) každé obmedzenie pri použití služby,
c) povinnosti Odberateľa, ak existujú,
d) informácie pre Spoliehajúce sa strany,
e) časové obdobie, počas ktorého Poskytovateľ uchováva záznamy o udalosti,
f) obmedzenia zodpovednosti,
g) obmedzenia pri použití poskytovanej služby, vrátane obmedzenia práva na náhradu škody vzniknutej pri použití služby spôsobom, prekračujúcim tieto obmedzenia,
h) aplikovateľnú legislatívu,
i) postupy pre vybavenie sťažností a urovnávanie sporov,
j) informáciu či dôveryhodná služba Poskytovateľa bola posúdená s ohľadom na súlad s politikou dôveryhodných služieb a ak áno, prostredníctvom akej schémy posudzovania,
k) kontaktné údaje Poskytovateľa.

Odberatelia a Spoliehajúce sa strany musia byť informované o všeobecných podmienkach, vrátane vyššie uvedených položiek, pred uzatvorením zmluvného vzťahu s Poskytovateľom.
Všeobecné podmienky musia byť Odberateľom a Spoliehajúcim sa stranám dostupné

prostredníctvom trvalých komunikačných prostriedkov v čitateľnom a zrozumiteľnom jazyku. Všeobecné podmienky môžu byť šírené elektronicky.

6.3. Politika informačnej bezpečnosti

Poskytovateľ musí mať definovanú politiku informačnej bezpečnosti, ktorá stanovuje prístup organizácie k riadeniu jej informačnej bezpečnosti a ktorá je schválená manažmentom Poskytovateľa.
Zmeny vykonané v politike informačnej bezpečnosti musia byť v prípade potreby oznámené tretím stranám. To zahŕňa Odberateľov, Spoliehajúce strany, hodnotiace, dozorné a iné regulačné orgány.
Povinnosti Poskytovateľa:

- Poskytovateľ musí mať zdokumentovanú, implementovanú a udržiavanú politiku informačnej bezpečnosti, vrátane riadenia bezpečnostných kontrol a prevádzkových postupov pre zariadenia, systémy a informačné prostriedky Poskytovateľa.
- Poskytovateľ musí publikovať a komunikovať politiku informačnej bezpečnosti všetkým zamestnancom, ktorých sa táto politika týka.
- Poskytovateľ preberá plnú zodpovednosť za súlad s postupmi predpísanými v politike informačnej bezpečnosti a to aj vtedy, ak funkcionalita Poskytovateľa 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 pre informačnú bezpečnosť (odstavec 7.3) Poskytovateľa musia byť posudzované v plánovaných intervaloch alebo v prípade vzniku významných zmien s cieľom zabezpečiť ich trvalú vhodnosť, primeranosť a účinnosť. Akékoľvek zmeny, ktoré môžu mať dopad, resp. môžu vplývať na poskytovanú úroveň zabezpečenia, schvaľuje riadiaci orgán na základe odstavca 6.1 ods. d). Konfigurácia systémov Poskytovateľa by mala byť pravidelne kontrolovaná na zmeny, ktoré môžu narušiť bezpečnostné politiky Poskytovateľa.

7. RIADENIE A PREVÁDZKA POSKYTOVATEĽA

7.1. Vnútorná organizácia

7.1.1. Spoľahlivosť organizácie

Poskytovateľ sa považuje za spoľahlivú organizáciu, keď:

a) Politiky a pravidlá dôveryhodnej služby, na základe ktorých Poskytovateľ pôsobí, sú nediskriminačné.
b) Služby Poskytovateľa sú prístupné všetkým Odberateľom, ktorých činnosti spadajú do oblasti pôsobnosti, a ktorí súhlasia s tým, že budú dodržiavať svoje povinnosti uvedené v zmluvných podmienkach Poskytovateľa.
c) 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.
d) Poskytovateľ má finančnú stabilitu a zdroje požadované na prevádzku v súlade s touto politikou.
e) 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.
f) Poskytovateľ má zdokumentovanú dohodu a zmluvný vzťah, ak poskytovanie služieb zahŕňa subdodávateľské zmluvy, outsourcing alebo iné dohody tretích strán.

7.1.2. Delenie povinností

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

7.2. Ľudské zdroje

Poskytovateľ zabezpečuje, že zamestnanci a zmluvní pracovníci podporujú dôveryhodnosť prevádzky Poskytovateľa a to nasledovne:

a) Poskytovateľ zamestnáva zamestnancov, 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 zamestnanca.
b) Zamestnanci Poskytovateľa sú schopní spĺňať požiadavky „odborných vedomostí, skúseností a kvalifikácie“ prostredníctvom formálneho vzdelávania, školení a certifikátov, prípadne prostredníctvom reálnych skúseností alebo kombináciou oboch.
c) V prípade porušenia politík a postupov Poskytovateľa zamestnancom sa uplatňujú primerané disciplinárne sankcie.
d) Bezpečnostné role a zodpovednosti (špecifikované v politike informačnej bezpečnosti Poskytovateľa) sú zdokumentované v popise práce alebo v dokumentoch dostupných všetkým zainteresovaným zamestnancom. Dôveryhodné role, na ktorých závisí bezpečnosť prevádzky Poskytovateľa sú jasne identifikované. Tieto role sú menované a akceptované manažmentom Poskytovateľa a osobou, ktorá v danej roli pracuje.
e) Zamestnanci (dočasní aj trvalí) majú definovaný popis práce z pohľadu rolí. Popis práce zohľadňuje delenie zodpovedností, minimálnych nárokov (odstavec 7.1.2), určuje citlivosť pracovnej pozície založenej na povinnostiach a úrovni prístupu, určuje úroveň požadovanej previerky, potrebné školenia a uvedomenie si ich zodpovednosti. Poskytovateľ tam kde je to vhodné rozlišuje medzi všeobecnými funkciami a špecifickými funkciami.
f) Zamestnanci poskytovateľa vykonávajú administratívne a manažérske postupy, ktoré sú v súlade s postupmi riadenia informačnej bezpečnosti Poskytovateľa.
g) Riadiaci pracovníci Poskytovateľa majú skúsenosti alebo odbornú prípravu, resp. školenia v súvislosti s dôveryhodnou službou, ktorá je Poskytovateľom poskytovaná. Riadiaci pracovníci sú oboznámení s bezpečnostnými postupmi určenými pre pracovníkov a majú skúsenosť s bezpečnostnými povinnosťami, s informačnou bezpečnosťou a s posudzovaním rizík. Tieto skúsenosti sú dostatočné pre vykonávanie riadiacej funkcie.
h) Zamestnanci Poskytovateľa, pracujúci v dôveryhodných rolách, sa nenachádzajú v konflikte záujmov, ktorý by mohol ovplyvniť nezaujatosť zamestnanca pri prevádzke dôveryhodných služieb Poskytovateľa.
i) Dôveryhodné role zahŕňajú nasledovné zodpovednosti:
    a. Bezpečnostný manažér – má celkovú zodpovednosť za správu a implementáciu bezpečnostných postupov.
    b. Systémový správca – inštaluje, konfiguruje a udržiava dôveryhodný systém Poskytovateľa z pohľadu riadenia služieb.
    c. Systémový operátor – má zodpovednosť za každodennú prevádzku dôveryhodného systému Poskytovateľa a zálohovanie systému.
    d. Systémový audítor – je autorizovaný na prezeranie archívov a auditných záznamov dôveryhodného systému Poskytovateľa.
j) Zamestnanci Poskytovateľa sú do dôveryhodných rolí formálne menovaní riadiacim zamestnancom Poskytovateľa.
k) Zamestnanci Poskytovateľa majú prístup k dôveryhodným funkciám až po vykonaní všetkých požadovaných a nevyhnutých kontrol.

7.3. Správa aktív

7.3.1. Všeobecné požiadavky

Poskytovateľ musí zabezpečiť vhodnú úroveň ochrany svojich aktív vrátane informačných aktív. Poskytovateľ musí udržiavať inventár/zoznam všetkých informačných aktív a musí aktíva klasifikovať v súlade s posúdením rizika.

7.3.2. Manipulácia s médiami

S každým médiom musí byť zaobchádzané bezpečne v zmysle požiadaviek klasifikačnej schémy informácií. Média obsahujúce citlivé údaje musia byť bezpečne zlikvidované, ak už nie sú ďalej potrebné.

7.4. Riadenie prístupu

Prístup do systému Poskytovateľa je obmedzený len pre autorizovaných jednotlivcov nasledovne:

a) Prvky ochrany (napr. firewall) chránia vnútornú sieť Poskytovateľa pred neoprávneným prístupom vrátane prístupu Odberateľov a tretích strán. Firewally sú nakonfigurované v záujme prevencie tak, že používajú len protokoly a prístupy nevyhnutné pre prevádzku Poskytovateľa.
b) Prístupy operátorov, administrátorov a audítorov systému sú spravované Poskytovateľom. Táto správa zahŕňa správu používateľských účtov a včasnú aktualizáciu alebo odstránenie prístupov.
c) 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 manažmentu bezpečnosti a prevádzky.
d) Zamestnanci Poskytovateľa sú identifikovaní a autorizovaní pred použitím kritických aplikácii, ktoré súvisia s dôveryhodnými službami.
e) Aktivity zamestnancov Poskytovateľa sú v rámci systému Poskytovateľa zaznamenávané.
f) Citlivé údaje sú chránené voči obnoveniu prostredníctvom opätovného použitia pamäťových objektov (napr. odstránených súborov), ktoré sú sprístupnené neoprávneným používateľom.

7.5. Kryptografické riadiace prvky

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

7.6. Fyzická a objektová bezpečnosť

Poskytovateľ riadi fyzický prístup ku komponentom systému Poskytovateľa, ktorých bezpečnosť je kritická pre poskytovanie dôveryhodných služieb a minimalizuje riziká súvisiace s fyzickou bezpečnosťou nasledovne:

a) Fyzický prístup ku komponentom systému Poskytovateľa, ktoré sú z pohľadu bezpečnosti kritické pre poskytovanie dôveryhodných služieb je obmedzený len pre oprávnených jednotlivcov.
b) Poskytovateľ má prijaté opatrenia:
    a. zabraňujúce strate, poškodeniu alebo kompromitovaniu aktív a prerušeniu obchodných aktivít.
    b. zabraňujúce kompromitovaniu alebo odcudzeniu informácií a prostriedkov spracovania informácií.
c) Komponenty kritické z pohľadu zabezpečenia prevádzky dôveryhodných služieb sú umiestnené v chránených bezpečných priestoroch, ktoré disponujú fyzickou ochranou proti vniknutiu. Bezpečné priestory majú zabezpečenú kontrolu prístupu s opatreniami pre prístup a alarm pre prípad detegovania prieniku.

7.7. Prevádzková bezpečnosť

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

a) V rámci každého projektu, ktorý vyvíja systém v mene Poskytovateľa, resp. pre Poskytovateľa, sú v etape návrhu a špecifikácie požiadaviek na systém analyzované požiadavky na bezpečnosť s cieľom zaistenia bezpečnosti vyvíjaného systému.

b) 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.
c) Úplnosť (integrita) informácii a systémov Poskytovateľa je chránená proti vírusom, malvérom a neoprávnenému prístupu.
d) S médiami používanými v systémoch poskytovateľa je zaobchádzané bezpečne, aby nedošlo k poškodeniu, odcudzeniu, neoprávnenému prístupu alebo zastaranosti média.
e) Poskytovateľ má postupy správy médií, ktoré chránia pred zastaranosťou a poškodením média v čase, počas ktorého je požadované uchovávanie týchto médií.
f) Poskytovateľ má stanovené a implementované postupy pre všetky dôveryhodné a administratívne role, ktoré sa podieľajú na poskytovaní služieb.
g) Poskytovateľ má špecifikované a aplikované postupy pre zabezpečenie:
    a. aplikovania bezpečnostných záplat v primeranom čase od kedy sú dostupné.
    b. neaplikovania bezpečnostných záplat, ktoré predstavujú ďalšiu zraniteľnosť alebo nestabilitu systému, ktoré prevažujú nad výhodami ich aplikovania. Dôvody neaplikovania bezpečnostnej záplaty sú zdokumentované.

7.8. Sieťová bezpečnosť

Poskytovateľ chráni svoju sieť a systémy pred útokom, najmä:
a) 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.
b) obmedzením prístupov a komunikácie medzi zónami len na nevyhnutné prípady z pohľadu zabezpečenia prevádzky Poskytovateľa. Nepotrebné prepojenia a služby je potrebné zakázať alebo deaktivovať a zavedený súbor pravidiel pravidelne posudzovať.
c) udržiavaním systémov, ktoré sú z pohľadu prevádzky Poskytovateľa kritické v jednej alebo viacerých bezpečných zónach.
d) oddelením dedikovaných sietí pre správu IT systémov a prevádzkových sietí Poskytovateľa. Nepoužívaním systémov, ktoré slúžia na správu implementácie bezpečnostnej politiky na iné účely a oddelením produkčného systému dôveryhodných služieb Poskytovateľa od systému používaného na vývoj a testovanie.
e) 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.
f) zabezpečením vysokej úrovne dostupnosti dôveryhodných služieb pre externé prístupy v prípade, že sa takáto dostupnosť vyžaduje, a to pomocou redundantného prístupu do siete, ktorý zabezpečí dostupnosť služby aj pri vzniku jednoduchej chyby.
g) vykonávaním pravidelného vyhľadávania zraniteľnosti na verejných aj súkromných IP, ktoré Poskytovateľ identifikoval 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 nevyhnutnú na poskytnutie hodnovernej správy.
h) vykonaním penetračných testov na systémoch Poskytovateľa po zriadení, aktualizácii alebo zmene, ktoré Poskytovateľ identifikuje ako podstatné. Poskytovateľ eviduje záznam o každom vykonanom penetračnom teste. Eviduje či bol realizovaný osobou alebo subjektom, ktorý má potrebné a požadované zručnosti, či boli použité vhodné nástroje, a či bol dodržaný etický kódex a nezávislosť, ktorá je nevyhnutná na poskytnutie hodnovernej správy.

7.9. Riadenie bezpečnostných incidentov

Systémové aktivity týkajúce sa prístupov a využívania IT systémov ako aj požiadavky na služby sú monitorované, keď:
a) Monitorovacie aktivity zohľadňujú citlivosť všetkých zbieraných a analyzovaných informácií.

b) Abnormálne systémové aktivity, ktoré naznačujú potenciálne porušenie bezpečnosti, vrátane vniknutia do siete Poskytovateľa, sú detegované a hlásené ako výstraha.
c) IT systém Poskytovateľa monitoruje nasledovné udalosti:
    a. spustenie a vypnutie logovacích funkcionalít,
    b. dostupnosť a využitie služieb v sieti Poskytovateľa.
d) V prípade vzniku incidentu Poskytovateľ koná včas a koordinovane s cieľom obmedziť dosah porušenia bezpečnosti. Poskytovateľ má menovaných zamestnancov v dôveryhodných rolách, ktorí sledujú výstrahy možných kritických bezpečnostných udalostí a zabezpečujú aby boli príslušné incidenty hlásené v súlade s postupmi Poskytovateľa.
e) Poskytovateľ má zavedené postupy pre informovanie príslušných strán v súlade s platnými regulačnými pravidlami o každom porušení bezpečnosti alebo strate integrity, ktorá má významný dopad na poskytované dôveryhodné služby a osobné údaje, ktoré sú v nej udržiavané, a to do 24 hodín od identifikácie porušenia.
f) Ak porušenie bezpečnosti, resp. strata integrity môže nepriaznivo ovplyvniť fyzickú alebo právnickú osobu, ktorej bola poskytnutá dôveryhodná služba, Poskytovateľ bezodkladne o tejto skutočnosti informuje dotknutú osobu.
g) Systémy Poskytovateľa sa monitorujú, vrátane monitorovania a pravidelného posudzovania auditných záznamov s cieľom identifikovať dôkazy o škodlivých aktivitách, a to implementovaním automatických mechanizmov na spracovanie auditných záznamov a informovanie personálu na možné kritické bezpečnostné udalosti.
h) Poskytovateľ rieši každú kritickú zraniteľnosť, ktorej sa predtým nevenoval, do 48 hodín od identifikovania tejto zraniteľnosti. Ak je to nákladovo efektívne, Poskytovateľ vytvorí a implementuje plán zmiernenia zraniteľnosti. V prípade, že zraniteľnosť nie je potrebné odstrániť, je vytvorená dokumentácia podkladov, ktorá viedla k takémuto rozhodnutiu.
i) Postupy hlásenia a reakčné postupy sú používané takým spôsobom, aby sa minimalizovali škody spôsobené bezpečnostnými incidentmi a poruchami.

7.10. Zber dôkazov

Poskytovateľ zaznamenáva a v primeranej dobe udržuje dostupné všetky relevantné informácie, týkajúce sa údajov vydaných a prijatých Poskytovateľom (aj v prípade, že Poskytovateľ už neposkytuje dôveryhodné služby). Doba uchovávania informácii o životnom cykle kľúčov je 10 rokov. Tieto úkony musí Poskytovateľ vykonávať pre prípad potreby poskytnutia dôkazov v súdnom konaní a zabezpečenia kontinuity služieb. Poskytovateľ spomenuté docieli:

a) udržiavaním dôvernosti a integrity súčasných a archivovaných záznamov týkajúcich sa prevádzky dôveryhodných služieb.
b) dôverným archivovaním záznamov týkajúcich sa prevádzky služieb. Archivácia záznamov je realizovaná v súlade so zverejnenými obchodnými praktikami.
c) sprístupnením záznamov týkajúcich sa dôverných služieb na účely poskytnutia dôkazu o správnom fungovaní služieb v prípade súdneho konania.
d) zaznamenávaním presného času významných udalostí Poskytovateľa v oblasti týkajúceho sa prostredia Poskytovateľa, správy kľúčov a synchronizácie hodín. Čas, ktorý sa používa na zaznamenávanie udalostí v protokole auditu, musí byť minimálne raz denne synchronizovaný s UTC.
e) uchovávaním záznamov týkajúcich sa služieb po dobu, ktorá je potrebná na poskytnutie potrebných právnych dôkazov a ktorá je oznámená v podmienkach Poskytovateľa (pozri odstavec 6.2).
f) Zaznamenáva udalosti tak, aby ich nebolo možné jednoducho odstrániť alebo zničiť (s výnimkou prípadu, keď sú spoľahlivo prenesené na dlhodobé média) a to v čase, keď sa vyžaduje ich uchovávanie.

7.11. Riadenie kontinuity činnosti organizácie

Poskytovateľ ma definovaný a udržiavaný plán kontinuity, ktorý bude prijatý v prípade vzniku pohromy. V prípade pohromy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých

údajov Poskytovateľa) musí byť prevádzka Poskytovateľa obnovená v rámci oneskorenia definovaného v pláne kontinuity.

7.12. Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

a) Poskytovateľ pred ukončením poskytovania svojich služieb aplikuje minimálne nasledovné postupy:
    a. Informuje o ukončení poskytovania služieb všetkých Odberateľov a iné entity, s ktorými má Poskytovateľ uzatvorené zmluvy alebo iné formy vzťahov. O ukončení poskytovania služieb informuje aj Spoliehajúce sa strany.
    b. Ukončí autorizáciu všetkých subdodávateľov, ktorí konali v zastúpení Poskytovateľa pri vykonávaní akýchkoľvek funkcií súvisiacich s procesom vydávania tokenov pre dôveryhodné služby.
    c. Prenesie všetky záväzky týkajúce sa uchovávania informácií potrebných na poskytovanie dôkazov o prevádzke Poskytovateľa počas primerane stanovenej doby na spoľahlivú stranu.
    d. Zničí (vrátane kópií) alebo stiahne z používania primárne kľúče takým spôsobom, že ich nebude možné znovu obnoviť a používať.
    e. Vytvorí dohodu (ak je to možné) o prevode poskytovania dôveryhodných služieb pre svojich súčasných Odberateľov na iného poskytovateľa dôveryhodných služieb.
b) Poskytovateľ je príspevková organizácia, z toho dôvodu je krytie nákladov na splnenie týchto minimálnych požiadaviek v prípade, že Poskytovateľ zanikne alebo z iných dôvodov nie je schopný pokryť náklady sám, zabezpečené štátnym rozpočtom.
c) Poskytovateľ vo svojich postupoch uvedie ustanovenia o ukončení poskytovania dôveryhodných služieb čo zahŕňa:
    a. informovanie všetkých dotknutých entít,
    b. prevod záväzkov Poskytovateľa na tretie strany.
d) Poskytovateľ bude dodržiavať svoje záväzky o sprístupnení svojho verejného kľúča alebo dôkazov o dôveryhodných službách Spoliehajúcim sa stranám počas primeranej doby, resp. prevedie tieto záväzky na inú dôveryhodnú osobu.

7.13. Zhoda

Poskytovateľ poskytuje služby dôveryhodným spôsobom a v rámci platnej legislatívy, aby:
a) mohol poskytnúť dôkaz, že spĺňa legislatívne požiadavky súvisiace s poskytovaním dôveryhodných služieb.
b) mohli byť dôveryhodné služby Poskytovateľa a s nimi súvisiace produkty poskytnuté aj osobám s telesným postihnutím.
c) prijal vhodné technické a organizačné opatrenia proti neoprávnenému spracovaniu osobných údajov a proti náhodnej strate, zničeniu alebo poškodeniu osobných údajov.

7.14. Orgán dohľadu

Poskytovateľ je povinný pri komunikácii s orgánom dohľadu v zmysle požiadaviek Nariadenia eIDAS a Zákona č. 272/2016 Z. z. o dôveryhodných službách:
a) ak Poskytovateľ zamýšľa začať poskytovať kvalifikované dôveryhodné služby predložiť orgánu dohľadu oznámenie o svojom zámere spolu so správou o posúdení zhody, ktorú vydal orgán posudzovania zhody,
b) poskytnúť úradu informácie o zmenách v jeho kvalifikovaných dôveryhodných službách najneskôr do 30 dní pred plánovanou zmenou,
c) zasielať orgánu dohľadu:
    a. vydané kvalifikované certifikáty pre kvalifikovaný elektronický podpis a pre kvalifikovanú elektronickú pečať do 30 dní od vydania kvalifikovaného certifikátu,
    b. potvrdenie o dátume a čase zrušenia kvalifikovaných certifikátov 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,

d) 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.