KCCKB Verejné

Druh dokumentu: Politika

POLITIKA POSKYTOVANIA DÔVERYHODNÝCH SLUŽIEB

Číslo: 20
Verzia: 2

Zverejnený: 27.5.2024
Účinný od: 27.5.2024

Záväzný pre: *VŠETCI ZAMESTNANCI*
Prístupný pre: *VEREJNOSŤ*

Vydal útvar: *Odbor auditu a konzultačných činností*
Autori: Tomáš Hettych, Marián Illovský
Spoluautori:

Schválil: Ivan Makatura, generálny riaditeľ

1 ÚVOD

Tento dokument špecifikuje politiku (ďalej len „PTSP“) Kompetenčného a certifikačného centra kybernetickej bezpečnosti so sídlom Na družstvo 125, 916 25 Brunovce , korešpondenčná adresa Budatínska 32, 851 06 Bratislava (ďalej aj „KCCKB“) ako poskytovateľa dôveryhodných služieb (ďalej len „TSP KCCKB“) a platí pre všetky ním poskytované dôveryhodné služby.

Politika definuje požiadavky, ktorých naplnenie je nevyhnutné uplatňovať v rámci riadenia a prevádzky TSP KCCKB.

Táto politika:

a) Vychádza z požiadaviek uvedených v dokumente ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers" [1];

b) Má všeobecný charakter a nemusí pokrývať všetky špecifické požiadavky kladené na jednotlivé poskytované dôveryhodné služby.

c) Nešpecifikuje ako majú byť jednotlivé požiadavky na TSP KCCKB posudzované nezávislými tretími stranami, vrátane požiadaviek na informácie, ktoré majú byť k dispozícii nezávislým posudzovateľom, alebo požiadavky na takýchto posudzovateľov.

Pokiaľ sú v tejto politike definované povinnosti TSP KCCKB ich právnym nositeľom je prevádzkovateľ tejto certifikačnej autority, ktorým je Kompetenčné a certifikačné centrum kybernetickej bezpečnosti.

1.1 Názov dokumentu a jeho identifikácia

Táto politika je identifikovaná nasledovným identifikátorom odvodeným od objektového identifikátora KCCKB:

1.3.158.52839052.0.1.1

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
52839052	jedinečný identifikátor KCCKB (IČO)
0	poskytovanie dôveryhodných služieb
1	Certifikačné politiky
1	Politika poskytovania dôveryhodných služieb

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".

3 DEFINÍCIE A SKRATKY

3.1 Definície

Použité pojmy sú prevzaté z 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 „Nariadenia eIDAS“) [2] a normy ETSI EN 319 401 [1].

Spoliehajúca sa strana	Ľubovoľná právnická alebo fyzická osoba, ktorá na základe overovania časovej pečiatky skúma (overuje alebo verifikuje) či údaje ku ktorým existuje časová pečiatka objektívne existovali v určitom (určiteľnom) čase.
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.
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

PTSP	Politika poskytovania dôveryhodných služieb
TSP KCCKB	Certifikačná autorita *(Certification Authority)* prevádzkovaná Kompetenčným a certifikačným centrom kybernetickej bezpečnosti

3.3 Všeobecné ustanovenia

Dôveryhodné služby, na ktoré sa vzťahuje táto politika sú:

- vyhotovovanie kvalifikovaných elektronických časových pečiatok

Tento dokument musí byť aktualizovaný najmä v nasledujúcich prípadoch:

- pri zmene prevádzkových podmienok,
- pri zmene procesov,
- pri zmene rizikového profilu alebo ako reakcia na bezpečnostné incidenty,
- alebo minimálne raz za 2 roky.

Za jeho aktualizáciu zodpovedá vlastník dokumentu.

4 POSÚDENIE RIZÍK

TSP KCCKB musí vykonať posúdenie rizík s cieľom identifikovať, analyzovať a vyhodnotiť riziká súvisiace s poskytovaním dôveryhodnej služby s ohľadom na obchodné a technické otázky.

TSP KCCKB 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.

TSP KCCKB 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.

Vedenie TSP KCCKB musí schváliť posúdenie rizík a akceptované zvyškové riziká.

5 POLITIKY A PRAKTIKY

5.1 Politiky a pravidlá pre poskytovanie dôveryhodných služieb

TSP KCCKB 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 TSP KCCKB:

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

5.2 Všeobecné podmienky

Všeobecné podmienky týkajúce sa služieb TSP KCCKB musia byť sprístupnené všetkým klientom a Spoliehajúcim sa stranám.

Tieto všeobecné podmienky musia špecifikovať pre politiku každej dôveryhodnej služby podporovanej TSP KCCKB minimálne:

- aplikovanú politiku dôveryhodnej služby
- každé obmedzenie pri použití služby (napr. doba platnosti certifikátu)
- povinnosti klienta, ak existujú
- informácie pre Spoliehajúce sa strany (napr. ako verifikovať token dôveryhodnej služby)
- časové obdobie, počas ktorého TSP KCCKB uchováva záznamy o udalosti

- 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 TSP KCCKB bola posúdená s ohľadom na súlad s politikou dôveryhodných služieb a ak áno, prostredníctvom akej schémy posudzovania
- kontaktné údaje TSP KCCKB

Klienti a Spoliehajúce sa strany musia byť informované o všeobecných podmienkach, vrátane vyššie uvedených položiek, pred uzatvorením zmluvného vzťahu s TSP KCCKB. Všeobecné podmienky musia byť klientom a Spoliehajúcim sa stranám dostupné prostredníctvom trvalých komunikačných prostriedkov v čitateľnom a zrozumiteľnom jazyku. Všeobecné podmienky môžu byť šírené elektronicky.

5.3 Politika informačnej bezpečnosti

TSP KCCKB musí mať definovanú politiku informačnej bezpečnosti, ktorá stanovuje prístup organizácie k riadeniu jej informačnej bezpečnosti a ktorá je schválená vedením TSP KCCKB.

Zmeny vykonané v politike informačnej bezpečnosti musia byť v prípade potreby oznámené tretím stranám. To zahŕňa klientov, Spoliehajúce strany, hodnotiace, dozorné a iné regulačné orgány.

Povinnosti TSP KCCKB:

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

6 RIADENIE A PREVÁDZKA TSP KCCKB

6.1 Vnútorná organizácia

6.1.1 Spoľahlivosť organizácie

TSP KCCKB sa považuje za spoľahlivú organizáciu, keď:

- Politiky a pravidlá dôveryhodnej služby, na základe ktorých TSP KCCKB pôsobí, sú nediskriminačné.
- Služby TSP KCCKB sú prístupné všetkým klientom, ktorých činnosti spadajú do oblasti pôsobnosti, a ktorí súhlasia s tým, že budú dodržiavať svoje povinnosti uvedené v zmluvných podmienkach TSP KCCKB.
- TSP KCCKB 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 TSP KCCKB.
- TSP KCCKB má finančnú stabilitu a zdroje požadované na prevádzku v súlade s touto politikou.
- TSP KCCKB má politiky a postupy na riešenie sťažností a sporov prijatých od klientov alebo Spoliehajúcich sa strán týkajúcich sa poskytovania služieb a/alebo iných súvisiacich záležitostí.
- TSP KCCKB má zdokumentovanú dohodu a zmluvný vzťah, ak poskytovanie služieb zahŕňa subdodávateľské zmluvy, outsourcing alebo iné dohody tretích strán.

6.1.2 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 TSP KCCKB.

6.2 Ľudské zdroje

TSP KCCKB zabezpečuje, že zamestnanci a zmluvní pracovníci podporujú dôveryhodnosť prevádzky TSP KCCKB a to nasledovne:

- TSP KCCKB 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.
- Zamestnanci TSP KCCKB 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 TSP KCCKB zamestnancom sa uplatňujú primerané disciplinárne sankcie.
- Bezpečnostné role a zodpovednosti (špecifikované v politike informačnej bezpečnosti TSP KCCKB) sú zdokumentované v popise práce alebo v dokumentoch dostupných všetkým zainteresovaným

zamestnancom. Dôverné role, na ktorých závisí bezpečnosť prevádzky TSP KCCKB sú jasne identifikované. Tieto role sú menované a akceptované vedením TSP KCCKB a osobou, ktorá v danej roli pracuje.

- 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. TSP KCCKB tam kde je to vhodné rozlišuje medzi všeobecnými funkciami a špecifickými funkciami.
- Zamestnanci TSP KCCKB vykonávajú administratívne a riadiace postupy, ktoré sú v súlade s postupmi riadenia informačnej bezpečnosti TSP KCCKB.
- Riadiaci pracovníci TSP KCCKB majú skúsenosti alebo odbornú prípravu, resp. školenia v súvislosti s dôveryhodnou službou, ktorá je TSP KCCKB 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.
- Zamestnanci TSP KCCKB, pracujúci v dôverných rolách, sa nenachádzajú v konflikte záujmov, ktorý by mohol ovplyvniť nezaujatosť zamestnanca pri prevádzke dôveryhodných služieb TSP KCCKB.
- Dôveryhodné role zahŕňajú nasledovné zodpovednosti:
    - Bezpečnostný správca – má celkovú zodpovednosť za správu a implementáciu bezpečnostných postupov.
    - Administrátor (OS) – inštaluje, konfiguruje a udržiava dôveryhodný systém TSP KCCKB z pohľadu riadenia služieb.
    - Operátori – má zodpovednosť za každodennú prevádzku dôveryhodného systému TSP KCCKB a zálohovanie systému.
    - Interný audítor – je autorizovaný na prezeranie archívov a auditných záznamov dôveryhodného systému TSP KCCKB.
- Zamestnanci TSP KCCKB majú prístup k dôveryhodným funkciám až po vykonaní všetkých požadovaných a nevyhnutých kontrol.

6.3 Správa aktív

6.3.1 Všeobecné požiadavky

TSP KCCKB musí zabezpečiť vhodnú úroveň ochrany svojich aktív vrátane informačných aktív.

TSP KCCKB musí udržiavať inventár/zoznam všetkých informačných aktív a musí aktíva klasifikovať v súlade s posúdením rizika.

6.3.2 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.

6.4 Riadenie prístupu

Prístup do systému TSP KCCKB je obmedzený len pre autorizovaných jednotlivcov nasledovne:

- Prvky ochrany (napr. firewall) chránia vnútornú sieť TSP KCCKB pred neoprávneným prístupom vrátane prístupu klientov a tretích strán. Firewally sú nakonfigurované v záujme prevencie tak, že používajú len protokoly a prístupy nevyhnutné pre prevádzku TSP KCCKB.
- Prístupy operátorov, administrátorov a audítorov systému sú spravované TSP KCCKB. Táto správa zahŕňa správu používateľských účtov a včasnú aktualizáciu alebo odstránenie prístupov.
- Prístup k informáciám a funkciám systému je obmedzený v zmysle politiky riadenia prístupu. Systém TSP KCCKB poskytuje vhodné prvky počítačovej bezpečnosti na oddelenie dôveryhodných rolí identifikovaných v postupoch TSP KCCKB. Oddelenie dôveryhodných rolí zahŕňa aj oddelenie funkcií manažmentu bezpečnosti a prevádzky.
- Zamestnanci TSP KCCKB sú identifikovaní a autorizovaní pred použitím kritických aplikácii, ktoré súvisia s dôveryhodnými službami.
- Aktivity zamestnancov TSP KCCKB sú v rámci systému TSP KCCKB zaznamenávané.
- Citlivé údaje sú chránené voči obnoveniu prostredníctvom opätovného použitia pamäťových objektov (napr. odstránených súborov), ktoré sú sprístupnené neoprávneným používateľom.

6.5 Kryptografické riadiace prvky

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

6.6 Fyzická a objektová bezpečnosť

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

- Fyzický prístup ku komponentom systému TSP KCCKB, ktoré sú z pohľadu bezpečnosti kritické pre poskytovanie dôveryhodných služieb je obmedzený len pre oprávnených jednotlivcov.
- TSP KCCKB má prijaté opatrenia:
    - Zabraňujúce strate, poškodeniu alebo kompromitovaniu aktív a prerušeniu obchodných aktivít.
    - Zabraňujúce kompromitovaniu alebo odcudzeniu informácií a prostriedkov spracovania informácií.

- 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.

6.7 Prevádzková bezpečnosť

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

- V rámci každého projektu, ktorý vyvíja systém v mene TSP KCCKB, resp. pre TSP KCCKB, sú v etape návrhu a špecifikácie požiadaviek na systém analyzované požiadavky na bezpečnosť s cieľom zaistenia bezpečnosti vyvíjaného systému.
- Pre nasadzovanie, zmenu, núdzové opravy alebo aktualizáciu konfigurácií akéhokoľvek systému TSP KCCKB, na ktorý sa aplikuje bezpečnostná politika sú použité postupy riadenia zmien. Tieto postupy zahŕňajú dokumentáciu realizovaných zmien.
- Úplnosť (integrita) informácii a systémov TSP KCCKB je chránená proti vírusom, malvérom a neoprávnenému prístupu.
- S médiami používanými v systémoch TSP KCCKB je zaobchádzané bezpečne, aby nedošlo k poškodeniu, odcudzeniu, neoprávnenému prístupu alebo zastaranosti média.
- TSP KCCKB má postupy správy médií, ktoré chránia pred zastaranosťou a poškodením média v čase, počas ktorého je požadované uchovávanie týchto médií.
- TSP KCCKB má stanovené a implementované postupy pre všetky dôveryhodné a administratívne role, ktoré sa podieľajú na poskytovaní služieb.
- TSP KCCKB 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.

6.8 Sieťová bezpečnosť

TSP KCCKB chráni svoju sieť a systémy 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. TSP KCCKB 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 TSP KCCKB. Nepotrebné prepojenia a služby je potrebné zakázať alebo deaktivovať a zavedený súbor pravidiel pravidelne posudzovať.

- Udržiavaním systémov, ktoré sú z pohľadu prevádzky TSP KCCKB kritické v jednej alebo viacerých bezpečných zónach.
- Oddelením dedikovaných sietí pre správu IT systémov a prevádzkových sietí TSP KCCKB. Nepoužívaním systémov, ktoré slúžia na správu implementácie bezpečnostnej politiky na iné účely a oddelením produkčného systému dôveryhodných služieb TSP KCCKB 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 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.
- Vykonávaním pravidelného vyhľadávania zraniteľnosti na verejných aj súkromných IP, ktoré TSP KCCKB 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.
- Vykonaním penetračných testov na systémoch TSP KCCKB po zriadení, aktualizácii alebo zmene, ktoré TSP KCCKB identifikuje ako podstatné. TSP KCCKB 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.

6.9 Riadenie bezpečnostných incidentov

Systémové aktivity týkajúce sa prístupov a využívania informačných systémov TSP KCCKB ako aj požiadavky na služby sú monitorované, keď:

- Monitorovacie aktivity zohľadňujú citlivosť všetkých zbieraných a analyzovaných informácií.
- Abnormálne systémové aktivity, ktoré naznačujú potenciálne porušenie bezpečnosti, vrátane vniknutia do siete TSP KCCKB, sú detegované a hlásené ako výstraha.
- IT systém TSP KCCKB monitoruje nasledovné udalosti:
    - Spustenie a vypnutie logovacích funkcionalít
    - Dostupnosť a využitie služieb v sieti TSP KCCKB
- V prípade vzniku incidentu TSP KCCKB koná včas a koordinovane s cieľom obmedziť dosah porušenia bezpečnosti. TSP KCCKB má menovaných zamestnancov v dôveryhodných rolách, ktorí sledujú výstrahy možných kritických bezpečnostných udalostí a zabezpečujú aby boli príslušné incidenty hlásené v súlade s postupmi TSP KCCKB.
- TSP KCCKB 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.

- Ak porušenie bezpečnosti, resp. strata integrity môže nepriaznivo ovplyvniť fyzickú alebo právnickú osobu, ktorej bola poskytnutá dôveryhodná služba, TSP KCCKB bezodkladne o tejto skutočnosti informuje dotknutú osobu.
- Systémy TSP KCCKB 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.
- TSP KCCKB rieši každú kritickú zraniteľnosť, ktorej sa predtým nevenoval, do 48 hodín od identifikovania tejto zraniteľnosti. Ak je to nákladovo efektívne, TSP KCCKB vytvorí a implementuje plán zmiernenia zraniteľnosti. V prípade, že zraniteľnosť nie je potrebné odstrániť, je vytvorená dokumentácia podkladov, ktorá viedla k takémuto rozhodnutiu.
- Postupy hlásenia a reakčné postupy sú používané takým spôsobom, aby sa minimalizovali škody spôsobené bezpečnostnými incidentmi a poruchami.

6.10 Zber dôkazov

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

- Udržiavaním dôvernosti a integrity súčasných a archivovaných záznamov týkajúcich sa prevádzky dôveryhodných služieb.
- Dôverným archivovaním záznamov týkajúcich sa prevádzky služieb. Archivácia záznamov je realizovaná v súlade so zverejnenými obchodnými praktikami.
- Sprístupnením záznamov týkajúcich sa dôverných služieb na účely poskytnutia dôkazu o správnom fungovaní služieb v prípade súdneho konania.
- Zaznamenávaním presného času významných udalostí TSP KCCKB v oblasti týkajúceho sa prostredia TSP KCCKB, správy kľúčov a synchronizácie hodín. Čas, ktorý sa používa na zaznamenávanie udalostí v protokole auditu, musí byť minimálne raz denne synchronizovaný s UTC.
- Uchovávaním záznamov týkajúcich sa služieb po dobu, ktorá je potrebná na poskytnutie potrebných právnych dôkazov a ktorá je oznámená v podmienkach TSP KCCKB.
- 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.

6.11 Riadenie kontinuity činnosti organizácie

TSP KCCKB ma definovaný a udržiavaný plán kontinuity, ktorý bude prijatý v prípade vzniku pohromy. V prípade pohromy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých údajov TSP KCCKB) musí byť prevádzka TSP KCCKB obnovená v rámci oneskorenia definovaného v pláne kontinuity.

6.12 Ukončenie činnosti TSP KCCKB a plány ukončenia činnosti

TSP KCCKB pred ukončením poskytovania svojich služieb aplikuje minimálne nasledovné postupy:

- Informuje o ukončení poskytovania služieb všetkých klientov a iné entity, s ktorými má TSP KCCKB uzatvorené zmluvy alebo iné formy vzťahov. O ukončení poskytovania služieb sa informujú aj Spoliehajúce sa strany.
- Ukončí autorizáciu všetkých subdodávateľov, ktorí konali v zastúpení TSP KCCKB 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 TSP KCCKB počas primerane stanovenej doby na spoľahlivú stranu.
- 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 klientov na iného TSP KCCKB dôveryhodných služieb.

Zriaďovateľ TSP KCCKB zabezpečí pokrytie nákladov na splnenie týchto minimálnych požiadaviek v prípade, že TSP KCCKB zanikne alebo z iných dôvodov nie je schopný pokryť náklady sám, a to s ohľadom na platnú legislatívu.

TSP KCCKB vo svojich postupoch uvedie ustanovenia o ukončení poskytovania dôveryhodných služieb čo zahŕňa:

- Informovanie všetkých dotknutých entít
- Prevod záväzkov TSP KCCKB na tretie strany

TSP KCCKB 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.

6.13 Zhoda

TSP KCCKB poskytuje služby dôveryhodným spôsobom a v rámci platnej legislatívy, aby:

- Mohol poskytnúť dôkaz, že spĺňa legislatívne požiadavky súvisiace s poskytovaním dôveryhodných služieb.
- Mohli byť dôveryhodné služby TSP KCCKB a s nimi súvisiace produkty poskytnuté aj osobám s telesným postihnutím.

- Prijal vhodné technické a organizačné opatrenia proti neoprávnenému spracovaniu osobných údajov a proti náhodnej strate, zničeniu alebo poškodeniu osobných údajov.

6.14 Orgán dohľadu

TSP KCCKB je povinný pri komunikácii s orgánom dohľadu v zmysle požiadaviek Nariadenia eIDAS a Zákona č. 272/2016 Z. z. o dôveryhodných službách:

- ak TSP KCCKB 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 vydania kvalifikovaného certifikátu (ak sú využívané),
    - 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.