



POLITIKA

poskytovania dôveryhodných
služieb



Disig, a.s.

Vypracoval	Peter Miškovič ; Petra Vydrová, Janka Pelešová
------------	--

Dátum	18.4.2017
-------	-----------

Verzia	1.0
--------	-----

Typ	POLITIKA
-----	----------

Schválil	Ľuboš Batěk
----------	--------------------

Obsah

1.	Úvod	3
1.1	Identifikácia	3
2.	Odkazy	4
3.	Definície a skratky	5
3.1	Definície	5
3.2	Skratky	6
4.	Všeobecné ustanovenia	7
5.	Posúdenie rizík	8
6.	Politiky a praktiky.....	9
6.1	Politky a pravidlá pre poskytovanie dôveryhodných služieb	9
6.2	Všeobecné podmienky	9
6.3	Politika informačnej bezpečnosti	10
7.	Riadenie a prevádzka Poskytovateľa	12
7.1	Vnútoraná organizácia	12
7.1.1	Spoľahlivosť organizácie	12
7.1.2	Delenie povinností	12
7.2	Ľudské zdroje	12
7.3	Správa aktív	14
7.3.1	Všeobecné požiadavky.....	14
7.3.2	Manipulácia s médiami	14
7.4	Riadenie prístupu	14
7.5	Kryptografické riadiace prvky	15
7.6	Fyzická a objektová bezpečnosť	15
7.7	Prevádzková bezpečnosť	15
7.8	Sieťová bezpečnosť	16
7.9	Riadenie bezpečnostných incidentov	17
7.10	Zber dôkazov.....	18
7.11	Riadenie kontinuity činnosti organizácie	18
7.12	Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti	19
7.13	Zhoda	19
7.14	Orgán dohľadu	20

1. Úvod

Tento dokument špecifikuje politiku spoločnosti Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísanú v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B, ako poskytovateľa dôveryhodných služieb (ďalej len „Poskytovateľ“) a platí pre všetky ním poskytované dôveryhodné služby.

Politika definuje požiadavky, ktorých naplnenie je nevyhnutné uplatňovať v rámci manažmentu a prevádzky Poskytovateľa.

Táto politika:

- Vychádza z požiadaviek uvedených v dokumente ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers" [1];
- Má všeobecný charakter a nemusí pokrývať všetky špecifické požiadavky kladené na jednotlivé poskytované dôveryhodné služby.
- 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

Názov:	Politika poskytovania dôveryhodných služieb
Skratka názvu:	TSP_P Disig
Verzia:	1.0
Schválené dňa:	11.4.2017
Platnosť od:	18.4.2017
Tomuto CP je priradený identifikátor objektu (OID):	1.3.158.35975946.0.1.0.0.1

Popis použitého identifikátora objektu (OID):

1 - ISO assigned OIDs

1.3 - ISO Identified Organization

1.3.158 - Identifikačné číslo subjektu (IČO)

1.3.158.35975946 - Disig

1.3.158.35975946.0.1 - Disig - dôveryhodný poskytovateľ služieb

1.3.158.35975946.0.1.0.0.1 - TSP_P Disig

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	3/21

2. Odkazy

[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".

Súbor	P_TSP_Disig	Verzia	1.0		
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana	4/21

3. Definície a skratky

3.1 Definície

Použité definície 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 európskej normy ETSI EN 319 401 [1]:

Univerzálny koordinovaný **čas** (Coordinated Universal Time (UTC)): časová škála založená na sekunde podľa definície v Recommendation ITU-R TF.460-6 [1], „svetový čas“.

Spoliehajúca sa strana: fyzická alebo právnická osoba spoliehajúca sa na elektronickú identifikáciu alebo dôveryhodnú službu.

Zákazník: právnická alebo fyzická osoba, ktorej povinnosti sú dané zmluvou s poskytovateľom dôveryhodnej služby.

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.

Politika dôveryhodnej služby: súbor pravidiel, ktoré indikujú použiteľnosť dôveryhodnej služby pre konkrétnu komunitu a/alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami.

Poskytovateľ dôveryhodných služieb: je fyzická alebo právnická osoba poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb; .

Token dôveryhodnej služby: fyzický alebo binárny (logický) objekt generovaný alebo vydaný ako výsledok použitia dôveryhodnej služby (napríklad: certifikát, CRL, časová pečiatka, OCSP odpoveď)

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 5/21

3.2 Skratky

Použité technické skratky:

CA	–	Certifikačná autorita, autorita vydávajúca certifikáty verejného kľúča (Certification Authority)
CA Disig	–	Certifikačná autorita prevádzkovaná Poskytovateľom
IP	–	Sieťový komunikačný protokol (Internet Protocol)
IT	–	Informačná technológia (Information Technology)
NBÚ	–	Národný bezpečnostný úrad
UTC	–	Koordinovaný univerzálny čas, svetový čas (Coordinated Universal Time)

4. Všeobecné ustanovenia

Dôveryhodné služby, na ktoré sa vzťahuje táto politika sú:

- vyhotovovanie a overovanie kvalifikovaných certifikátov pre elektronický podpis
- vyhotovovanie a overovanie kvalifikovaných certifikátov pre elektronickú pečať
- vyhotovovania a overovania kvalifikovaných certifikátov pre autentifikáciu webových sídiel
- validácia kvalifikovaných elektronických podpisov
- validácia kvalifikovaných elektronických pečatí
- uchovávanie kvalifikovaných elektronických podpisov
- uchovávanie kvalifikovaných elektronických pečatí
- vyhotovovanie kvalifikovaných elektronických časových pečiatok

5. Posúdenie rizík

Poskytovateľ musí **vykonať** posúdenie rizík, aby identifikoval, analyzoval a vyhodnotil riziká poskytovania dôveryhodnej služby z pohľadu obchodných a technických otázok.

Poskytovateľ musí **zvoliť** primerané opatrenia na riadenie rizík **vzhľadom** na výsledky posúdenia rizík. Opatrenia na riadenie rizík musia **zabezpečiť**, že úroveň bezpečnosti bude primeraná definovanej miere rizika.

Pri riadení rizík **informačnej bezpečnosti**, ako súčasť systému riadenia **informačnej bezpečnosti**, musí **vychádzať** z požiadaviek ISO/IEC 27005. [3]

Poskytovateľ musí **mať** zvolené **bezpečnostné** požiadavky a prevádzkové postupy potrebné na implementáciu opatrení riadenia rizík. Tieto musia **byť** dokumentované v politike **informačnej bezpečnosti** a v pravidlách na vykonávanie dôveryhodných služieb.

Posúdenie rizík musí **byť** pravidelne prehodnocované a aktualizované.

Posúdenie rizík a akceptovanie identifikovaných zvyškových rizík musí **schváliť** manažment **Poskytovateľa**.

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	8/21

6. Politiky a praktiky

6.1 Politky a pravidlá pre poskytovanie dôveryhodných služieb

Poskytovateľ musí špecifikovať súbor politík a pravidiel vhodných pre poskytované dôveryhodné služby. Tieto musia byť schválené manažmentom, publikované a komunikované so zamestnancami a externými stranami podľa dôležitosti.

Poskytovateľ musí mať pravidlá a postupy pre poskytované dôveryhodné služby, a to predovšetkým:

- Pravidlá a postupy pokrývajúce všetky požiadavky identifikované aplikovateľnou politikou Poskytovateľa dostupné Zákazníkom a Spoliehajúcim sa stranám spolu s ďalšou relevantnou dokumentáciou, ak je to nutné k posúdeniu zhody s politikou služby;;
- Pravidlá identifikujúce záväzky všetkých externých organizácií, ktoré podporujú služby TSP, vrátane aplikovateľných politík a pravidiel;

Ďalej musí mať

- určený manažment s celkovou zodpovednosťou za dôveryhodné služby a oprávnený schvaľovať politiky a pravidlá pre poskytovanie dôveryhodných služieb;
- určený manažment zodpovedný za implementáciu politík a pravidiel;
- definované postupy preskúmania politík a pravidiel vrátane zodpovednosti za ich udržovanie;
- postupu upozorňovania na zamýšľané zmeny v politikách a pravidlách a po ich schválení postupy ich prístupnosti;
- definované politiky a pravidlá a opatrenia, ktoré budú prijaté v prípade ukončenia poskytovania dôveryhodnej služby.

6.2 Všeobecné podmienky

Poskytovateľ musí sprístupniť všeobecné podmienky týkajúce sa jeho služieb všetkým odberateľom a spoliehajúcim sa stranám.

Tieto všeobecné podmienky musia špecifikovať pre každú politiku dôveryhodných služieb podporovaných Poskytovateľom nasledovné:

- aplikovanú politiku dôveryhodných služieb;
- obmedzenia v použití služby (napr. doba platnosti certifikátu);
- záväzky odberateľa;
- informáciu pre Spoliehajúce sa strany (napr. ako verifikovať token služby, akékoľvek možné obmedzenia doby platnosti spojené s tokenom dôveryhodnej služby);

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	9/21

- e) dobu uchovávanía záznamu udalostí (event log);
- f) obmedzenie zodpovednosti;
- g) obmedzenia použitia poskytovanej služby vrátane obmedzenia práva na náhradu škody vzniknutej pri použití služby spôsobom, ktorý prekračuje tieto obmedzenia;
- h) rozhodné právo;
- i) procedúry pre riešenie sťažností a sporov;
- j) či dôveryhodná služba **Poskytovateľa** bola predmetom posúdenia zhody s politikou dôveryhodnej služby a ak, prostredníctvom akej schémy posudzovania (conformity assessment scheme);
- k) kontaktné informácie **Poskytovateľa**;

Zákazníci musia byť pred poskytnutím dôveryhodnej služby informovaní o Všeobecných podmienkach ako aj obmedzeniach použitia poskytovanej služby. Všeobecné podmienky musia byť prístupné na trvanlivom médiu (v papierovej forme, resp. vo formáte pdf na webovom sídle **Poskytovateľa**) a musia byť písané v ľahko pochopiteľnom jazyku.

6.3 Politika informačnej bezpečnosti

Poskytovateľ musí mať definovanú politiku informačnej bezpečnosti schválenú manažmentom spoločnosti, ktorá definuje prístup **Poskytovateľa** k riadeniu informačnej bezpečnosti, kde hlavne musí:

- a) **Mať** zdokumentovanú, implementovanú a udržiavanú politiku informačnej bezpečnosti, vrátane riadenia bezpečnostných opatrení a prevádzkových postupov pre zariadenia, systémy a informačné aktíva **Poskytovateľa** využívané na poskytovanie dôveryhodných služieb. Politiku informačnej bezpečnosti musí publikovať a zdieľať so všetkými zamestnancami, ktorých sa týka.
- b) **Prebrať** plnú zodpovednosť za zhodu s procedúrami predpísanými v politike informačnej bezpečnosti aj v prípade, že funkcionality **Poskytovateľa** je zabezpečovaná dodávateľsky. **Poskytovateľ** musí mať definované záväzky pre dodávateľov a musí zabezpečiť, že dodávatelia sú zviazaní implementovať akékoľvek riadiace prvky požadované **Poskytovateľom**.
- c) **Preskúmať** politiku informačnej bezpečnosti a zoznam aktív pre informačnú bezpečnosť (odstavec 7.3) v plánovaných intervaloch, alebo ak nastanú významné zmeny z dôvodu udržateľnosti jej vhodnosti, prijateľnosti a efektívnosti. Akékoľvek zmeny, ktoré môžu vplyvať na úroveň poskytovanej bezpečnosti, musia byť schválené manažmentom (odstavec 6.1 a)). Konfigurácia systémov **Poskytovateľa** musí byť pravidelne kontrolovaná z dôvodov zmien, ktoré môžu narušiť bezpečnostnú politiku **Poskytovateľa**.

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 10/21

Zmeny v politike informačnej bezpečnosti musia byť v prípade potreby komunikované tretím stranám, čo zahŕňa Zákazníkov, Spoliehajúce sa strany, orgány posudzovania, dozorné a iné regulačné orgány.

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	11/21

7. Riadenie a prevádzka Poskytovateľa

7.1 Vnútorná organizácia

7.1.1 Spoľahlivosť organizácie

Poskytovateľa je spoľahlivá organizácia, čo preukazuje hlavne tým, že:

- a) politiky a pravidlá pre poskytovanie dôveryhodných služieb Poskytovateľa sú nediskriminačné;
- b) **s**ristupňuje svoje služby všetkým Zákazníkom, ktorých aktivity spadajú do deklarovanej oblasti použitia, a ktorí súhlasia s dodržiavaním záväzkov špecifikovaných vo Všeobecných podmienkach Poskytovateľa;
- c) má vhodné **f**inančné zdroje a vhodné poistenie zodpovednosti za škodu, ktorá pokrýva jeho prevádzkové resp. iné aktivity;
- d) má **f**inančnú stabilitu a zdroje požadované na prevádzku v súlade s touto politikou.
- e) má politiky a procedúry na riešenie **s**tážností a sporov so Zákazníkmi alebo inými Spoliehajúcimi sa stranami, ktoré sa týkajú poskytovaných služieb alebo iných súvisiacich záležitostí.
- f) má uzavreté písomné zmluvy so **s**ubdodávateľmi v prípadoch, že poskytovanie jeho služieb je **z**abezpečované prostredníctvom **s**ubdodávateľov, poskytovateľov služby outsourcingu alebo iných tretích strán.

7.1.2 Delenie povinností

Povinnosti alebo oblasti zodpovednosti, ktoré sú v konflikte, sú oddelené aby sa obmedzili príležitosti pre neautorizovanú alebo neúmyselnú modifikáciu alebo zneužitie aktív Poskytovateľa.

7.2 Ľudské zdroje

Poskytovateľ **z**abezpečuje, aby zamestnanci a zmluvní pracovníci podporovali dôveryhodnosť prevádzky Poskytovateľa hlavne tým, že:

- a) Zamestnáva pracovníkov, ktorí:
 - majú potrebné odborné znalosti, **s**poľahlivosť, skúsenosti a kvalifikáciu,
 - absolvovali školenie týkajúce sa **z**ebezpečnosti resp. ochrany osobných údajov primerané pre nimi poskytované služby a pracovnú poýiciu resp. pridelenú rolu;
- b) Sú schopní **s**plňať požiadavky na expertné znalosti, skúsenosti a kvalifikáciu prostredníctvom formálneho školenia a certifikátu, alebo reálnou **s**kúsenosťou, alebo kombináciou obidvoch;

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 12/21

- c) V prípade porušenia politiky resp. procedúr **Poskytovateľa** sú voči zamestnancom uplatňované adekvátne disciplinárne opatrenia;
- d) **Bezpečnostné** roly a zodpovednosti ako sú špecifikované v politike **informačnej bezpečnosti Poskytovateľa**, sú dokumentované aj v popise prác resp. v dokumentácii dostupnej všetkým zainteresovaným zamestnancom, ktorých sa to týka. **Dôveryhodné** roly, na ktorých závisí **bezpečnosť** prevádzky **Poskytovateľa**, sú jasne definované. **Dôveryhodné** roly sú menované a akceptované manažmentom a osobou, ktorá pracuje v tejto role;
- e) Zamestnanci **Poskytovateľa** majú popis práce, ktorý zohľadňuje princíp delenia zodpovedností, minimálnych nárokov (odstavec 7.1.2), **citlivosť** pozície **vzhľadom** na zodpovednosti a **úroveň prístupu**, **úroveň požadovanej** previerky, potrebné školenia a uvedenie si ich zodpovednosti;
- f) Zamestnanci vykonávajú administratívne a riadiace postupy a procesy, ktoré sú v súlade s postupmi riadenia **informačnej bezpečnosti Poskytovateľa**.
- g) Riadiaci zamestnanci majú skúsenosti alebo školenia zamerané na poskytované dôveryhodné služby, sú oboznámení s **bezpečnostnými** postupmi určenými pre zodpovedné osoby a majú skúsenosti s **informačnou bezpečnosťou** a posudzovaním rizík, ktoré sú **dostatočné** na výkon riadiacej funkcie.
- h) Všetci zamestnanci **Poskytovateľa** v dôveryhodných rolách sú mimo konfliktu záujmov, aby nemohlo **dôjsť** k porušeniu princípu nezaujatosti prevádzky **Poskytovateľa**.
- i) **Dôveryhodné** roly sú roly s nasledovnými **zodpovednosťami**:
- **Bezpečnostný manažér**: Majú celkovú **zodpovednosť** za riadenie a implementáciu **bezpečnostných** praktík.
 - **Systémový administrátor**: Je autorizovaný na inštalovanie, konfigurovanie a udržovanie dôveryhodného systému **Poskytovateľa** z pohľadu riadenia služieb.
 - **Administrátor systému CA a RA**: Je zodpovedný za prevádzku dôveryhodného systému **Poskytovateľa** na každodennej báze.
 - **Interný audítor**: Je autorizovaný na pozeranie archívov a auditných záznamov systémov **Poskytovateľa**.
- j) Zamestnanci **Poskytovateľa** sú do dôveryhodných rolí formálne menovaní členom manažmentu **Poskytovateľa**.
- k) Zamestnanci **Poskytovateľa** nemajú prístup k dôveryhodným funkciám, **pokiaľ** nie sú vykonané všetky nevyhnutné kontroly.

7.3 Správa aktív

7.3.1 Všeobecné požiadavky

Poskytovateľ musí **zabezpečiť** primeranú úroveň ochrany aktív vrátane informačných aktív.

Poskytovateľ musí **mať** zoznam všetkých informačných aktív s priradenou klasifikáciu v zmysle posúdenia rizík.

7.3.2 Manipulácia s médiami

So všetkými médiami musí **byť** manipulované **bezpečne** v zmysle požiadaviek klasifikačnej schémy informácií. Média obsahujúce citlivé údaje musia **byť**, v prípade nepotrebnosti, **bezpečne** likvidované.

7.4 Riadenie prístupu

Prístup do systémov **Poskytovateľa** musí **byť** obmedzený len pre autorizovaných jednotlivcov a to hlavne tým že:

- a) Riadiace prvky (napr. firewally) musia **chrániť** **oblasť** internej siete **Poskytovateľa** pred neautorizovaným prístupom, vrátane prístupu **odberateľov** a tretích strán. Firewally musia **byť** nakonfigurované tak, aby nepoužívali protokoly a prístupy, ktoré nie sú potrebné pre prevádzku **Poskytovateľa**.
- b) **Používateľský** prístup operátorov, administrátorov a audítorov systému musí **byť** spravovaný. Riadenie musí zahŕňať správu používateľských účtov a včasnú modifikáciu alebo zrušenie prístupu.
- c) Prístup k informáciám a funkciám **aplikačných** systémov musí **byť** obmedzený v zmysle politiky riadenia prístupov. Systémy **Poskytovateľa** musia **poskytovať** vhodné riadiace prvky **počítačovej bezpečnosti** na separáciu dôveryhodných rolí, ktoré sú identifikované v praktikách **Poskytovateľa**, vrátane oddelenia funkcií manažmentu **bezpečnosti** a prevádzkových funkcií.
- d) Zamestnanci **Poskytovateľa** musia **byť** pred použitím kritických aplikácií spojených so službami identifikovaní a autentifikovaní.
- e) Aktivity zamestnancov **Poskytovateľa** vykonávané v IS **Poskytovateľa** musia **byť** zaznamenávané.
- f) Citlivé údaje musia **byť** chránené **voči** obnoveniu pomocou opätovného použitia **pamäťových** objektov (napríklad vymazaných súborov) prístupných neautorizovaným **užívateľom**.

7.5 Kryptografické riadiace prvky

Musia byť použité primerané bezpečnostné opatrenia na správu akýchkoľvek kryptografických kľúčov a akýchkoľvek kryptografických zariadení v priebehu ich životného cyklu.

7.6 Fyzická a objektová bezpečnosť

Poskytovateľ musí riadiť fyzický prístup ku kritickým komponentom systému Poskytovateľa, ktoré slúžia pre poskytovanie jeho dôveryhodných služieb a minimalizovať riziká spojené s fyzickou bezpečnosťou a to hlavne:

- Fyzický prístup ku komponentom systému Poskytovateľa, ktorých bezpečnosť je kritická pre poskytovanie dôveryhodných služieb, musí byť obmedzená len na autorizovaných jednotlivcov;
- Musia byť prijaté opatrenia na zabránenie straty, zničenia alebo kompromitovania aktív resp. prerušenia obchodných aktivít;
- Musia byť prijaté opatrenia na zabránenie kompromitovania alebo krádeže informácií a prostriedkov spracovávajúcich informácie;
- Kritické komponenty slúžiace pre zabezpečenie prevádzky dôveryhodných služieb musia byť umiestnené v bezpečných priestoroch, ktoré sú chránené proti fyzickému prieniku, musia mať zabezpečenú kontrolu prístupu s opatreniami pre prístup cez bezpečnostný periméter a technickým zabezpečením s alarmom pri detegovaní prieniku.

7.7 Prevádzková bezpečnosť

Poskytovateľ musí používať dôveryhodné systémy a produkty, ktoré sú chránené proti modifikácii a zabezpečujú technickú bezpečnosť a spoľahlivosť nimi podporovaných procesov a to hlavne:

- V rámci vývoja akéhokoľvek systému pre Poskytovateľa resp. v mene Poskytovateľ musí byť už vo fáze návrhu vykonávaná analýza bezpečnostných požiadaviek, aby bola zaistená bezpečnosť budovaného systému.
- Pre vydávanie, modifikácie a núdzové opravy akéhokoľvek prevádzkového softvéru a na zmeny v konfigurácii, na ktoré sa aplikuje bezpečnostná politika Poskytovateľa, musia byť použité procedúry riadenia zmien. Procedúry musia zahŕňať dokumentáciu týchto zmien.
- Integrita systémov a informácií Poskytovateľa musí byť chránená proti vírusom, malvéru a neautorizovaným softvérom.
- S použitými médiami v systémoch Poskytovateľa musí náležať bezpečne tak, aby boli médiá chránené pred zničením, krádežou neautorizovaným prístupom a zastarávaním.

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 15/21

- e) Musia **byť** k dispozícii procedúry pre správu médií, ktoré ich chránia proti zastarávaniu a poškodeniu počas doby nevyhnutnej na uchovávanie na nich uložených záznamov.
- f) Musia **byť** stanovené a implementované postupy pre všetky dôveryhodné a administratívne roly, ktoré vplyvajú na poskytovanie služieb.
- g) **Poskytovateľ v rámci bezpečnosti:**
 - musí aplikovať bezpečnostné záplaty v rámci primeraného času od doby, keď sú dostupné;
 - neaplikovať bezpečnostné záplaty ak predstavujú ďalšiu zraniteľnosť alebo nestabilitu, ktorá preváži nad výhodami ich aplikácie;
 - musí dokumentovať dôvody pre neaplikovanie akýchkoľvek bezpečnostných záplat.

7.8 Sieťová bezpečnosť

Poskytovateľ musí chráni svoju sieť a systémy pred útokom, a to najmä nasledovnými spôsobmi:

- a) **Deliť** svoje systémy do zón podľa posúdenia rizík vzhľadom na funkčné, logické a fyzické vzťahy medzi dôveryhodnými systémami a službami.
- b) **Aplikovať** tie isté bezpečnostné prvky na všetky systémy umiestnené v tej istej zóne.
- c) **Obmedziť** prístup do zón a komunikáciu medzi zónami iba na tie, ktoré sú nevyhnutné pre prevádzku **Poskytovateľa**. Nepotrebné spojenia a služby výslovne **zakázať** alebo **deaktivovať**. Platné pravidlá pravidelne **prehodnocovať**.
- d) **Udržovať** všetky kritické systémy pre prevádzku **Poskytovateľa** v jednej alebo viacerých **zabezpečených zónach**.
- e) **Vyhradenú sieť** pre správu IT systémov a prevádzkovú sieť **Poskytovateľa oddeliť**. Systémy použité pre správu implementácie bezpečnostnej politiky nesmú **byť** použité pre iné účely. **Produkčné** systémy pre služby **Poskytovateľa** musia **byť** oddelené od systémov využívaných na vývoj a testovanie.
- f) Komunikácia medzi rozdielnymi dôveryhodnými systémami musí **byť** iba cez dôveryhodné kanály, ktoré sú logicky oddelené od iných **komunikačných kanálov** a poskytujú **zaručenú** identifikáciu ich koncových bodov a ochranu údajov v jednotlivých kanáloch pred modifikáciou alebo prezradením.
- g) Ak je vyžadovaná vysoká **dostupnosť** vybraných dôveryhodných služieb z **pohľadu** externého prístupu musí **byť** prístup do siete internet redundantným, aby bola zaistená **dostupnosť** služieb aj v prípade jednoduchej poruchy.

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	16/21

- h) **Vykonávať** pravidelné skúmanie zraniteľnosti na určených verejných alebo privátnych IP adresách infraštruktúry **Poskytovateľa** a **viest'** evidenciu, kým bolo toto skúmanie zraniteľnosti vykonané, aké nástroje boli použité, či bol dodržaný etický kódexu a **nezávislosť**, ktoré sú nevyhnutné na poskytnutie hodnovernej správy.
- i) Pri zriadení a po aktualizácii alebo modifikácii infraštruktúry **vykonávať** **penetračný test** určených systémov **Poskytovateľa** a **viest'** evidenciu, kým bol **penetračný test** vykonaný, aké nástroje boli použité, či bol dodržaný etický kódexu a **nezávislosť**, ktoré sú nevyhnutné na poskytnutie hodnovernej správy

7.9 Riadenie **bezpečnostných** incidentov

Systémové aktivity týkajúce sa prístupu k IT systémom, **používateľa** IT systémov ich použitie a požiadavky na služby musia **byť** monitorované. Platí, že:

- a) Monitorovacie aktivity musia **brať ohľad** na **citlivosť** zbieraných alebo analyzovaných informácií.
- b) Abnormálne aktivity systému, ktoré indikujú potenciálne narušenie **bezpečnosti** vrátane prieniku do siete **Poskytovateľa**, musia **byť** detegované a hlásené ako výstraha.
- c) IT systémy **Poskytovateľa** musia **monitorovať** nasledovné udalosti:
 - spustenie a vypnutie funkcií zaznamenávania udalostí;
 - **dostupnosť** a využitie potrebných služieb v sieti **Poskytovateľa**.
- d) **Poskytovateľ** musí **konať** **včasným** a koordinovaným spôsobom v záujme rýchlejšej odpovede na incidenty a obmedzenia vplyvu narušenia **bezpečnosti**. **Poskytovateľ** musí **určiť** personál v dôveryhodných rolách na sledovanie výstrah na potenciálne kritické **bezpečnostné** udalosti a **zabezpečenie**, aby prípadné incidenty boli hlásené v súlade s procedúrami **Poskytovateľa**.
- e) **Poskytovateľ** musí **mať** stanovené procedúry na notifikovanie príslušných strán v súlade s platnými pravidlami regulátora o **akomkoľvek** narušení **bezpečnosti** alebo strate integrity, ktoré má významný vplyv na poskytovanú dôveryhodnú službu resp. na spracovávané osobné údaje do 24 hodín od identifikácie porušenia.
- f) Ak narušenie **bezpečnosti** alebo strata integrity môže nepriaznivo **ovplyvniť** fyzickú alebo právnickú osobu, ktorej bola poskytovaná dôveryhodná služba, **Poskytovateľ** musí bez **zbytočného odkladu** **notifikovať** aj túto fyzickú alebo právnickú osobu o narušení **bezpečnosti** alebo strate integrity.
- g) Systémy **Poskytovateľa** musí **byť** monitorované vrátane monitorovanie alebo pravidelného posudzovania auditných záznamov na identifikovanie dôkazov **zlomyseľnej** aktivity implementovaním automatického mechanizmu na spracovanie auditných záznamov a upozornením personálu na možné kritické **bezpečnostné** udalosti.

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 17/21

- h) **Poskytovateľ** sa musí **zaoberať** akoukoľvek kritickou zraniteľnosťou, ktorej sa predtým nevenoval, najneskôr do 48 hodín po jej objavení. V prípade, že sa to javí rentabilnejšie vzhľadom k dopadu zraniteľnosti, môže byť vytvorený a implementovaný plán na jej **potlačenie**. V prípade vyhodnotenia, že **zraniteľnosť** nie je potrebné odstrániť, sú zdokumentované podklady vedúce k takémuto rozhodnutiu.
- i) Hlásenie incidentov a **reakčné** procedúry musia byť používané takým spôsobom, aby bola minimalizovaná škoda a **nefunkčnosti** v dôsledku bezpečnostných incidentov.

7.10 Zber dôkazov

Poskytovateľa musí **zaznamenávať** a primeraný čas **uchovávať** všetky relevantné informácie, ktoré sa týkajú údajov vydaných a prijatých **Poskytovateľom**, a to aj po **ukončení** poskytovania dôveryhodných služieb. Uvedené musí **vykonávať** za účelom poskytovania dôkazov v súdnom konaní a **zabezpečenia** kontinuity služieb. Docieli to najmä tým, že:

- a) Bude **udržiavať dôvernosc** a integritu aktuálnych aj archivovaných záznamov týkajúcich sa prevádzky služieb.
- b) Bude **archivovať** všetky záznamy týkajúce sa prevádzky služieb v zhode so zverejnenými obchodnými praktikami a **zabezpečuje** ich **dôvernosc**.
- c) Záznamy týkajúce sa prevádzky služieb budú dostupné, ak sú požadované pre poskytovanie dôkazov správnej prevádzky služieb v súdnom konaní.
- d) Bude sa **zaznamenávať** presný čas významných udalostí týkajúcich sa prostredia **Poskytovateľa**, správy kľúčov a synchronizácie hodín. Čas použitý na zaznamenávanie udalostí musí byť synchronizovaný s UTC minimálne raz denne, v zmysle požiadavky pre auditné záznamy (log).
- e) Záznamy týkajúce sa služieb bude uchováva počas dostatočne dlhého časového obdobia po vypršaní platnosti kľúčov alebo akéhokoľvek tokenu dôveryhodnej služby, a to za účelom poskytnutia potrebného dôkazu pre právne účely a ako to avizoval v politikách resp. prehláseniach o politikách **Poskytovateľa** (pozri odstavec 7.2).
- f) Udalosti musia byť zaznamenávané takým spôsobom, aby nemohli byť ľahko vymazané alebo **zničené počas** celej doby ich povinného uloženia.

7.11 Riadenie kontinuity činnosti organizácie

Poskytovateľ musí **definovať** a **udržiavať** plán kontinuity činnosti pre použitie v prípade pohromy. V prípade pohromy, čo zahrňuje aj kompromitáciu súkromného podpisového kľúča alebo kompromitáciu iných citlivých údajov **Poskytovateľa**, musí byť prevádzka obnovená v rámci oneskorenia, stanoveného v pláne kontinuity činnosti.

Súbor	P_TSP_Disig	Verzia	1.0	
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana 18/21

7.12 Ukončenie činnosti Poskytovateľa a plány ukončenia činnosti

Poskytovateľ musí minimalizovať riziko pre Zákazníkov a Spoliehajúce sa strany, ktoré by mohlo byť spôsobené ukončením poskytovania svojich služieb hlavne tým, že:

- a) Bude mať aktuálny plán pre prípad ukončenia poskytovania svojich služieb.
- b) Predtým, ako ukončí svoje služby dodrží minimálne nasledujúce procedúry:
 - Bude informovať o ukončení poskytovania svojich služieb všetkých Zákazníkov a iné entity, s ktorými má zmluvy alebo iné formy vzťahov; Táto informácia bude daná na vedomie aj Spoliehajúcim sa stranám.
 - Ukončí autorizáciu všetkých subdodávateľov konajúcich v zastúpení Poskytovateľa vo vykonávaní akýchkoľvek funkcií vzťahujúcich sa na proces vydávania tokenov dôveryhodnej služby.
 - Prevedie záväzky týkajúce sa uchovávanie všetkých informácií nevyhnutných na poskytovanie dôkazov o prevádzke Poskytovateľa počas primeranej doby na spoľahlivú stranu.
 - Súkromné kľúče, vrátane ich záloh, zničí alebo stiahne z používania takým spôsobom, že už nikdy nebudú môcť byť obnovené.
 - Pokúsi sa vytvoriť, ak to bude možné, dohodu o prevode poskytovania dôveryhodných služieb pre existujúcich zákazníkov na iného poskytovateľa dôveryhodných služieb.
- c) Bude mať prijaté opatrenia na pokrytie nákladov na splnenie týchto minimálnych požiadaviek pre prípad, že sa dostane do úpadku, alebo, že pre iné dôvody nebude schopný pokryť náklady sám, a to v rámci obmedzení platnej slovenskej legislatívy týkajúcej sa úpadku.
- d) Stanoví vo vlastných praktikách podmienky pre ukončenie poskytovania služieb, ktoré budú zahŕňať:
 - oznámenie dotknutým entitám; a
 - prevod záväzkov Poskytovateľa na tretie strany.
- e) Bude dodržiavať svoj záväzok zverejniť svoj verejný kľúč alebo tokeny svojich dôveryhodných služieb spoliehajúcim sa stranám počas primeranej doby, resp. previedie tento záväzok na inú dôveryhodnú osobu.

7.13 Zhoda

Poskytovateľ musí poskytovať svoje služby v súlade s právom a dôveryhodným spôsobom hlavne z dôvodu, aby:

- a) Mohol poskytnúť dôkaz o skutočnosti ako splňa platné právne požiadavky kladené na poskytované služby.

Súbor	P_TSP_Disig	Verzia	1.0
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017
		Strana	19/21

- b) Poskytované dôveryhodné služby a **používateľské** produkty použité na poskytovanie týchto služieb mohli **byť** prístupné pre osoby s telesným postihnutím.
- c) Prijal vhodné technické a **organizačné** opatrenia proti neautorizovanému alebo protiprávnemu spracovávaní osobných údajov a proti strate, **zničeniu** alebo poškodeniu osobných údajov.

7.14 Orgán **dohľadu**

Poskytovateľ musí pri komunikácii s orgánom **dohľadu** v zmysle požiadaviek Nariadenia eIDAS a Zákona č. 272/2016 Z.z. o dôveryhodných službách:

- **pokiaľ 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,
- **zasielat'** vydané kvalifikované certifikáty pre kvalifikovaný elektronický podpis a pre kvalifikovanú elektronickú **pečať** do 30 dní od vydania kvalifikovaného certifikátu,
- **zasielat'** potvrdenie o dátume a **čase** zrušenia kvalifikovaných certifikátov do 30 dní od ich zrušenia,
- **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,
- **zasielat'** 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,

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

Súbor	P_TSP_Disig	Verzia	1.0		
Typ	Politika (OID: 1.3.158.35975946.0.1.0.0.1)	Dátum	18.4.2017	Strana	20/21

História zmien

Verzia	Dátum	Popis revízie; revidoval
1.0	11.4.2017	Prvá verzia dokumentu; V zmysle Nariadenia eIDAS a ETSI EN 319 401; Miškovič; Vydrová, Pelešová