POLITIKA

Kvalifikovaná služba – OBELISK Validator QTS

Verze	1.1
Datum	13. května 2020
Autor	Petr Dolejší
Počet stran	32

verze 1.1 - PUBLIC

Upozornění

Tento veřejný dokument je určen pro potřebu společnosti SEFIRA spol. s r.o. a obsahuje politiku provozu kvalifikované služby OBELISK Validator QTS pro ověřování platnosti el. podpisů a pečetí. Převzetím a seznámením se s tímto dokumentem uživatel souhlasí s tím, že žádná část tohoto dokumentu nesmí být kopírována, a to v žádné podobě bez předchozího souhlasu firmy SEFIRA spol. s r.o. jako poskytovatele služby.

Autorská práva

V dokumentu je použito názvů firem a produktů, které mohou být chráněny patentovými a autorskými právy nebo mohou být registrovanými obchodními značkami podle příslušných ustanovení právního řádu.

verze 1.1 - PUBLIC

Historie změn

Datum	Platnost od	Verze	Status	Schválil
23.1.2019		0.1	Interní draft	
25.1.2019		0.2	Sjednocení pojmu Služba	
1.3.2019		0.3	Předfinální verze	
25.3.2019	**1.4.2019**	1.0	Finální schválená verze	Řídící orgán
15.5.2020	**15.6.2020**	1.1	Upřesnění autentizace Klientů o podporu autentizačních certifikátů, upřesnění definice Rozhraní Služby	Řídící orgán

verze 1.1 - PUBLIC

OBSAH

verze 1.1 - PUBLIC

verze 1.1 - PUBLIC

Seznam obrázků

Nenalezena položka seznamu obrázků.

verze 1.1 - PUBLIC

SOUVISEJÍCÍ DOKUMENTACE

Aktuální dokument neobsahuje žádné prameny.

část I

POLITIKA KVALIFIKOVANÉ SLUŽBY OBELISK VALIDATOR QTS

1. ÚVOD

Tento dokument uvádí pravidla a postupy, které společnost SEFIRA spol. s r.o. uplatňuje v souladu splatnými předpisy a technickými normami pro provoz služby pro ověřování elektronických podpisů a pečetí založených na kvalifikovaných certifikátech OBELISK Validator (dále jen OBELISK Validator nebo „Uznávaná služba“).

Tento dokument uvádí pravidla a postupy, které společnost SEFIRA spol. s r.o. uplatňuje v souladu splatnými předpisy a technickými normami pro provoz kvalifikované služby pro ověřování kvalifikovaných elektronických podpisů a pečetí OBELISK Validator QTS (dále jen „OBELISK Validator QTS“ nebo „Kvalifikovaná služba“).

Uznávaná služba provozovaná společností SEFIRA spol. s r.o. resp. Kvalifikovaná služba provozovaná společností SEFIRA spol. s r.o. jako kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dále též obecně jako „Služba“ není-li statut rozhodující), zajišťující ověřování elektronických podpisů a pečetí koncovým uživatelům a spoléhajícím se stranám (dále jen „Klient“) je poskytována všem Klientům na základě uzavřeného smluvního vztahu (dále jen „Smlouva“).

1.1 Přehled

Předmětem tohoto dokumentu je definovat politiku k poskytování Služby (dále „Politika“). Politika popisuje podmínky a nezbytné postupy, vztahujícími se ke Službě s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti.

Dodržení postupů a podmínek uvedených v této Politice zajišťuje, aby spoléhající se strany obdržely výsledek postupu ověření platnosti automatizovaným způsobem, který je spolehlivý, účinný a je opatřen zaručenou elektronickou pečetí poskytovatele kvalifikované služby ověřování platnosti podpisů a pečetí.

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Politika kvalifikované služby ověřování platnosti elektronických podpisů a pečetí, verze 1.1 - PUBLIC
OID politiky:	není přiděleno
Datum vydání:	15. června 2020
Doba platnosti:	Do odvolání nebo do dne ukončení provozu Služby

1.3 Participující subjekty

1.3.1 Poskytovatel Služby

Společnost SEFIRA spol. s r.o. jako poskytovatel služeb vytvářejících důvěru pro Uznávanou službu OBELISK Validator.

Společnost SEFIRA spol. s r.o. jako kvalifikovaný poskytovatel služeb vytvářejících důvěru po uveřejnění na příslušném Trust Listu pro Kvalifikovanou službu OBELISK Validator QTS.

1.3.2 Spoléhající se strany

Spoléhající se stranou je jakýkoli subjekt (fyzická osoba, právnická osoba nebo organizační složka státu), který uzavřel s poskytovatelem služby, společností SEFIRA spol. s r.o., smlouvu o využívání Služby dle této Politiky.

1.3.3 Amazon

Amazon.com je poskytovatel infrastruktury pro provoz prostředí Služby a poskytuje záruku pro bezpečné prostředí pro zpracování dat a jejich ukládání v souladu s požadavky kladenými na ochranu osobních údajů a lokalitu, kde jsou data uložena. Veškerá data Služby jsou ukládána a archivována na území Evropské unie.

1.3.4 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, orgán dohledu a další, kterým to podle platné legislativy přísluší.

1.4 Použití Služby

1.4.1 Přípustné použití Služby

Službu smí využívat pouze uživatelé, kteří se seznámili s touto Politikou, v souladu s garantovaným použitím Služby, pro účely procesů ověřování platnosti elektronických podpisů a pečetí.

Službu je možné čerpat pouze prostřednictvím definovaných Rozhraní a aplikací, které jsou Klientovi Poskytovatelem zpřístupněny.

1.4.1.1 Rozhraní

Uživatel Služby je povinen chránit rozhraní pro použití Služby proti neoprávněnému použití a zajistit odpovídající bezpečnost při používání Služby. Toto platí pro jakékoliv rozhraní, prostřednictvím kterého je Služba čerpána (dále jen „Rozhraní“).

Tímto Rozhraním jsou myšleny zejména webové služby pro integraci na Službu, jakékoliv aplikační či integrační rozhraní dodané výhradně Poskytovatelem Služby nebo jím určeným partnerem.

1.4.2 Omezení použití Služby

Službu dle této Politiky je možné využívat pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy a touto Politikou.

Za nepovolené použití Služby nenese její Poskytovatel žádnou odpovědnost. V případě porušení bezpečnosti či integrity Rozhraní nenese Poskytovatel Služby jakoukoliv odpovědnost za škody jakéhokoliv druhu způsobené použitím tohoto nezabezpečeného, podvrženého či jakkoliv porušeného Rozhraní.

1.5 Správa politiky

1.5.1 Organizace spravující Politiku

Za správu této Politiky je odpovědný provozovatel SEFIRA spol. s r.o. zastoupený pro tento účel ředitelem společnosti SEFIRA.

1.5.2 Kontaktní osoba organizace spravující Politiku

Kontaktní osobou pro věci týkající se této certifikační politiky je Manažer bezpečnosti Služby.

1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů služeb vytvářejících důvěru

Rozhodnutí o shodě je plně v kompetenci ředitele společnosti SEFIRA spol. s r.o.

1.5.4 Postupy pro schvalování Politiky

Ředitel společnosti SEFIRA spol. s r.o. stanovuje všechny postupy pro schvalování této Politiky a přípravu nových verzí. Tato osoba také schvaluje jednotlivé verze a jejich aktualizace.

1.6 Přehled použitých pojmů a zkratek

Pojem nebo zkratka	Vysvětlení
AdES	Advanced Electronic Signature – zaručený elektronický podpis splňující požadavky článku 26 Nařízení (EU) 90/2014
autentizační certifikát	v tomto dokumentu certifikát sloužící pro autentizaci přístupu ke Službě
AWS	Amazon Web Services – cloudové služby poskytovatele Amazon.com provozované v několika samostatných a izolovaných datových centrech v rámci EU
certifikát	v tomto dokumentu kvalifikovaný certifikát pro elektronické podpisy nebo pečetě
CRL	Certification Revocation List – seznam zneplatněných certifikátů. Obsahuje certifikáty, které nadále nelze pokládat za platné například z důvodu prozrazení odpovídajícího soukromého klíče subjektu. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou.
ČSN	označení českých technických norem
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
elektronická pečeť	v tomto dokumentu elektronická pečeť, resp. zaručená elektronická pečeť, resp. uznávaná elektronická pečeť, resp. kvalifikovaná elektronická pečeť dle platné legislativy
elektronický podpis	v tomto dokumentu elektronický podpis, resp. zaručený elektronický podpis, resp. uznávaný elektronický podpis, resp. kvalifikovaný elektronický podpis dle platné legislativy
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie

IS	informační systém
Klient	Spoléhající se strana
Kvalifikovaná služba	Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí je kvalifikovaná služba vytvářející důvěru vytvořená a provozovaná kvalifikovaným poskytovatelem vytvářejícím důvěru SEFIRA pro ověřování kvalifikovaných elektronických podpisů a pečetí dle specifikací ETSI
legislativa	aktuálně platná legislativa ČR včetně nařízení eIDAS
LoTL	List of Trusted Lists - EU: Seznam zveřejněný podle čl. 2 odst. 4 rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu, ve znění rozhodnutí Komise 2010/425/EU a prováděcího rozhodnutí Komise 2013/662/EU, který obsahuje informace oznámené členskými státy v souladu s čl. 2 odst. 3 rozhodnutí Komise 2009/767/ES.
OBELISK Validator QTS	Kvalifikovaná služba vytvářející důvěru pro ověřování platnosti kvalifikovaných elektronických podpisů a pečetí poskytovaná kvalifikovaným poskytovatelem služeb vytvářejících důvěru SEFIRA
OCSP	Online Certificate Status Protocol – protokol pro online ověření platnosti certifikátu dle RFC 6960
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
orgán dohledu	orgán dohledu nad dodržováním legislativy spojené s poskytováním služeb vytvářejících důvěru dle nařízení eIDAS
otisk	unikátní datový řetězec o neměnné délce, který je vypočítán z libovolných vstupních dat; jednoznačně reprezentuje vstupní data, tj. neexistuje stejný otisk pro dvě různé zprávy
PKI	Public Key Infrastructure – infrastruktura veřejných klíčů
POE	Proof Of Existence – jednoznačný časový údaj poskytující důkaz existence ověřovaných dat v čase, ke kterému je prováděna validace
Politika	tento dokument politiky provozu Služby pro ověřování elektronických podpisů a pečetí
Poskytovatel	Poskytovatel Služby ověřování platnosti elektronických podpisů a pečetí, společnost SEFIRA spol. s r.o.
QTS	Qualified Trusted Service – kvalifikovaná služba vytvářející důvěru
QTSP	Qualified Trust Service Provider – kvalifikovaný poskytovatel služeb vytvářejících důvěru

Rozhraní	Aplikační rozhraní pro čerpání Služby – jakékoliv rozhraní určené poskytovatelem Služby pro její čerpání, zejména webové služby pro integraci, jakákoliv aplikační či integrační rozhraní dodané výhradně Poskytovatelem Služby nebo jím určeným partnerem.
SEFIRA	Společnost SEFIRA spol. s r.o. jako Poskytovatel, TSP nebo QTSP
Služba	obecné označení pro poskytovanou službu ověřování platnosti elektronických podpisů a pečetí není-li rozhodující dotčená její varianta – Uznávaná služba nebo Kvalifikovaná služba
Smlouva	text smlouvy v elektronické nebo listinné podobě pro přístup ke Službě
soukromý klíč	souhrnné označení dat pro vytváření elektronického podpisu či pečeti, dat pro dešifrování a dat pro autentizaci
Spoléhající se strana	subjekt spoléhající se při své činnosti na výsledek ověření platnosti elektronického podpisu a elektronické pečeti
TL	Trusted List – důvěryhodný seznam podle nařízení eIDAS je pokračováním důvěryhodných seznamů podle rozhodnutí Komise 2009/767/ES. Obsahuje informace, které orgány dohledu jednotlivých států vydávají proto, aby bylo možné správně vyhodnotit typ, stav a právní účinky služeb vytvářejících důvěru v souladu s platnou legislativou.
TS	Trust Service – služba vytvářející důvěru
TSP	Trust Service Provider – poskytovatel služeb vytvářejících důvěru
Uznávaná služba	Služba ověřování platnosti elektronických podpisů a pečetí založených na kvalifikovaných certifikátech je služba vytvořená a provozovaná SEFIRA pro ověřování zaručených elektronických podpisů a pečetí založených na kvalifikovaných certifikátech dle specifikací ETSI v roli TSP
veřejný klíč	souhrnné označení dat pro ověřování elektronického podpisu a dat pro šifrování
WS	Web Services – technologie vzdáleného volání funkcí v distribuovaných systémech založená na protokolu pro vzdálená volání SOAP a jazyku pro popis poskytovaných služeb WSDL
ZoSVD	Zákon o službách vytvářejících důvěru pro elektronické transakce č. 297/2016 Sb.

verze 1.1 - PUBLIC

2. ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

SEFIRA zřizuje a provozuje interní úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Služba ověřování elektronických podpisů je poskytována jako veřejná Uznávaná služba. Poskytovatelem služby vytvářející důvěru je SEFIRA.

SEFIRA poskytuje tuto službu také jako QTSP po zveřejnění na příslušném TL v režimu Kvalifikovaná služba. Tato skutečnost je vždy jasně oznámena uživateli. Dále též v dokumentu této Politiky obecně jako „Služba“.

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti SEFIRA, případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:
  SEFIRA spol. s r.o.
  Antala Staška 2027/77
  140 00 Praha 4
  Česká republika
- internetová adresa http://www.sefira.cz.

Elektronická adresa, která slouží pro kontakt veřejnosti se SEFIRA, je validator@obelisk.cz.

Na výše uvedené internetové adrese lze získat informace o Službě https://www.sefira.cz/obelisk-validator-qts/.

2.3 Periodicita zveřejňování informací

Politika je zveřejňována po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu a zahájením provozu Služby dle nové Politiky.

Jakékoliv změny v používání Služby jsou oznámeny klientům prostřednictvím kontaktních údajů klientem uvedených.

Jakékoliv změny v poskytování Služby, včetně záměru o ukončení činnosti oznámí orgánu dohledu (Ministerstvo vnitra ČR) v souladu s eIDAS, článkem 24, odstavec 2, paragraf a).

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje SEFIRA bezplatně bez omezení.

verze 1.1 - PUBLIC

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům SEFIRA, nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

verze 1.1 - PUBLIC

3. IDENTIFIKACE A AUTENTIZACE

3.1 Počáteční ověření identity

Služba je dostupná pouze pro subjekty, které mají uzavřenu platnou smlouvu o využívání této služby (dále též „Smlouva“).

3.1.1 Registrace uživatele Služby

Osoby oprávněné pro získání přístupu ke Službě jsou uvedeny ve Smlouvě. Tyto oprávněné osoby mohou požádat o přidělení osobních autentizačních údajů pro přístup ke Službě.

3.1.2 Registrace IS jako klienta Služby

Osoby oprávněné pro získání přístupu ke Službě jsou uvedeny ve Smlouvě. Tyto oprávněné osoby mohou požádat o přidělení autentizačních údajů pro automatizovaný přístup ke Službě prostřednictvím webových služeb.

3.2 Autentizace ke Službě

Autentizace přístupu uživatele nebo IS ke Službě je možná pouze prostřednictvím Rozhraní pomocí přidělených autentizačních údajů. Autentizačními údaji pro Službu mohou být buď kombinace uživatelské jméno a heslo nebo autentizační certifikát vydaný Poskytovatelem Služby.

3.3 Ukončení čerpání Služby

V případě nedodržování podmínek pro využívání Služby definovaných v této Politice je Poskytovatel oprávněn pozastavit přístup uživatele k této Službě. V případě závažných pochybení je Poskytovatel oprávněn ukončit uživateli přístup ke Službě.

Pozastavení přístupu uživatele ke Službě je uživateli oznámeno způsobem uvedeným ve Smlouvě. V případě ukončení přístupu ke Službě je toto oznámeno způsobem uvedeným ve Smlouvě.

3.4 Rušení uživatelských účtů

Rušení uživatelských účtů ke Službě se provádí:

- na základě písemné žádosti oprávněné osoby uvedené ve Smlouvě;
- automaticky v případě ukončení Smlouvy.

4. POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY OBELISK VALIDATOR QTS

Služba zpracovává na svém vstupu celý dokument podepsaný dle technických specifikací a norem definovaných ETSI na něž je odkazováno z Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a prostřednictvím příslušných prováděcích aktů.

Vstupem Služby je pouze Rozhraní dodané a poskytnuté Poskytovatelem. Konzumováním Služby jiným způsobem, než je definováno Poskytovatelem, není povoleno a je vnímáno jako porušení podmínek poskytování Služby.

4.1 Uzavření Smlouvy

4.1.1 Subjekty oprávněné uzavřít Smlouvu

O uzavření Smlouvy může požádat jakýkoli subjekt (fyzická osoba, právnická osoba nebo organizační složka státu).

4.2 Technické parametry Služby

4.2.1 Ověřované certifikáty

Služba provádí ověřování elektronických podpisů a pečetí založených na kvalifikovaných certifikátech dle nařízení eIDAS.

Kvalifikovanost jednotlivých kvalifikovaných certifikátů, resp. kvalifikovaných poskytovatelů služeb vytvářejících důvěru, kteří tyto kvalifikované certifikáty vydaly, je ověřována vůči důvěryhodným seznamů (Trusted Lists). Seznam adres vš ech publikovaných TL členských států je zveřejněn Evropskou komisí v „seznamu TL“ (LoTL – List of Trusted Lists). Ten je dostupný ve strojově zpracovatelné formě na adrese:

- https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

4.2.2 Ověřované formáty podpisů a pečetí

Služba poskytuje ověřování platnosti elektronických podpisů a pečetí ve formátech uvedených v prováděcím aktu Evropské komise (EU) 2015/1506 ze dne 8. září 2015. Jmenovitě se jedná o následující formáty:

- PAdES – formát využívaný pro podepsání/pečetění PDF a PDF/A dokumentů dle technické specifikace ETSI TS 103 172, resp. ETSI EN 319 142
- XAdES – formát využívaný pro podepsání/pečetění strukturovaných dokumentů s datovou XML strukturou dle technické specifikace ETSI TS 103 171, resp. ETSI EN 319 132
- CAdES – formát využívaný pro podepsání/pečetění obecných binárních dat a dokumentů, u kterých není možné použít vložený podpis dle technické specifikace ETSI TS 103 173, resp. ETSI EN 319 122

- ASiC – formát pro kontejner s přidruženým podpisem/pečetí dle technické specifikace ETSI TS 103 174, resp. ETSI EN 319 162-1

Služba dále podporuje následující formáty dokumentů:

- Formáty MS Office 2007 (docx, xlsx, pptx) a MS Office 97-2003 (doc, xls, ppt), formát OpenDocument 1.2
- Formáty MS Office 2010 a novější (docx, pptx, xlsx)
- Formát S/MIME v3 – RFC 2632, RFC 3850, RFC 5750, RFC 5751

4.3 Validační proces

Jednotlivé typy podpisů a pečetí v podporovaných formátech dle kapitoly 4.2.2 umožňují různou úroveň ověřování platnosti elektronického podpisového/pečetícího certifikátu. Z toho důvodu Služba obsahuje různé validační procesy dle typu podpisu/pečeti a informací v něm obsažných.

Validační procesy identifikují kvalifikované a zaručené elektronické podpisy a pečeti. Potvrdí platnost kvalifikovaného elektronického podpisu a pečeti, pokud vyhovuje podmínkám definovaných v nařízení eIDAS, Článek 32.

Režim využití jako Kvalifikované služba OBELISK Validator QTS je vždy určen použitím určené validační politiky **Kvalifikovaná služba OBELISK Validator QTS** (resp. její identifikací **urn:sefira:obelisk:validation:policy:qes**).

Vlastní validační proces probíhá v souladu s požadavky ETSI EN 319 102-1 a dále pro jednotlivé formáty v souladu s ETSI TS 103 172 a ETSI EN 319 142 pro formát PAdES, ETSI TS 103 171 a ETSI EN 319 132 pro formát XAdES, ETSI TS 103 173 a ETSI EN 319 122 pro formát CAdES, ETSI TS 103 174 a ETSI EN 319 162 pro formát ASiC.

V režimu Uznávané služby lze využít libovolnou nabízenou politiku.

4.3.1 Výsledek validačního procesu

Pokud jsou elektronický podpis nebo pečeť dokumentu porušeny, je validační proces pozastaven a dále již není v ověřování atributů elektronického podpisu či pečeti pokračováno a validace je ukončena s výsledkem chyby o porušení podpisu či pečeti.

Výsledek validačního procesu může nabývat hodnot:

- Platný (TOTAL_PASSED)
- Neplatný (TOTAL_FAILED)
- Neurčitý (INDETERMINATE)

Vyhodnocení procesu validace elektronického podpisu či pečeti je přímo závislé na zvolené validační politice. Součástí výstupních dat a reportů jsou podrobné informace, na základě kterých bylo rozhodnuto o výsledku validačního procesu.

Validační proces je závislý na času posouzení, ke kterému je ověřování prováděno. Pokud je čas posouzení zadán uživatelem, je za takovýto údaj odpovědný uživatel Služby a tím i za interpretaci výsledku ověřování, které je platné k tomuto zadanému časovému okamžiku. V případě neuvedení požadovaného času posouzení je pro vyhodnocení ověření použit časový okamžik prokazatelné existence (POE) dokumentu, který může být buď:

- čas přijetí dokumentu Službou k ověření nebo
- kvalifikované elektronické časové razítko v rámci dokumentu.

4.3.2 Výstup validačního procesu

Služba poskytuje výstup validačního procesu ve formátu strukturovaných XML dat pro integraci do aplikací třetích stran a dále také jako PDF dokument s lidsky čitelným výstupem výsledku validačního procesu. Uživatel Služby si prostřednictvím jejího Rozhraní může zvolit, jaký výstup požaduje.

Vlastní odpověď Rozhraní Služby je z důvodů autenticity a ověřitelnosti odpovědi Služby zabezpečena zaručenou elektronikou pečetí Poskytovatele.

4.3.2.1 Strukturovaná XML data

Pro integraci do navazujících informačních systémů nabízí Služba výstup ve 3 typech výstupních XML dokumentů, které si může uživatel při volání Služby zvolit. Dodatečně je možné stáhnout i ostatní typy výstupních formátů.

Simple_report.xml obsahuje pouze základní zjednodušené informace o provedeném procesu ověření platnosti elektronických podpisů a pečetí pro všechny podpisy, pečeti a časová razítka v rámci dokumentu. Tento výstupní dokument neobsahuje zaručenou elektronickou pečeť.

Detailed_report.xml obsahuje podrobné informace o provedení a vyhodnocení všech kroků provedených v rámci validačního procesu pro všechny podpisy, pečeti a časová razítka v rámci dokumentu. Tento výstupní dokument neobsahuje zaručenou elektronickou pečeť.

Diagnostic_data.xml obsahuje všechny informace, na základě kterých bylo rozhodnuto o výsledku validačního procesu pro všechny podpisy, pečeti a časová razítka v rámci dokumentu. Mezi tyto informace např. patří informace o všech použitých certifikátech, důvěryhodných kotvách, CRL či OCSP odpovědi. Tento výstupní dokument je vždy opatřen zaručenou elektronickou pečetí Poskytovatele ve formátu XAdES.

4.3.2.2 PDF dokument

Pro snazší prezentaci výsledků validačního procesu koncovým uživatelům nabízí Služba výstup ve formátu PDF, který přehlednou grafickou formou umožňuje prezentovat průběh a výsledek validačního procesu. Služba nabízí dva typy výstupních PDF reportů, které svým obsahem odpovídají základním strukturovaným XML datům dle kapitoly 4.3.2.1

Simple_report.pdf obsahuje v grafické podobě informace v rozsahu dat odpovídajících strukturovanému XML výstupu **simple_report.xml**, který je spolu se strukturovaným XML výstupem **diagnostic_data.xml** vložen do dokumentu jako příloha. Tento výstupní dokument je vždy opatřen zaručenou elektronickou pečetí Poskytovatele.

Detailed_report.pdf obsahuje v grafické podobě podrobné informace v rozsahu dat odpovídajících kombinaci strukturovaného XML výstupu **simple_report.xml** a **detailed_report.xml**, které jsou spolu se strukturovaným XML výstupem **diagnostic_data.xml** vloženy do dokumentu jako přílohy. Tento výstupní dokument je vždy opatřen zaručenou elektronickou pečetí Poskytovatele.

4.4 Dostupnost Služby

Dostupnost Služby je garantována v režimu 365 x 24 hodin s výjimkou nutných odstávek pro správu a údržbu systému. Dále je z této dostupnosti vyjmuta doba potřebná pro obnovu Služby po havárii, na kterou neměl provozovatel Služby vliv a nemohl ji nijak ovlivnit.

Poskytovatel garantuje vysokou spolehlivost Služby, v rámci svých služeb a aplikací, které používají významní klienti a také infrastrukturou Amazon, v rámci které je Služba provozována.

Poskytovatel poskytuje garantovanou minimální dostupnost ukotvenou ve Smlouvě o poskytování Služby s koncovým Klientem.

4.5 Úschova dat pro ověřování platnosti elektronických podpisů a pečetí

Doba, po kterou jsou uchovávány soubory potřebné pro ověření platnosti elektronických podpisů a pečetí, činí minimálně 10 let.

verze 1.1 - PUBLIC

5. MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

- systém poskytované Služby a
- veškeré procesy podporující poskytování Služby.

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Bezpečnostní politika Služby, Havarijní plány a plán obnovy, tak v upřesňujících interních dokumentech.

Uvedené dokumenty reflektují výsledky periodicky prováděné Analýzy rizik.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Technologie Služby je umístěna a provozována v prostředí cloudu AWS společnosti Amazon.com. Toto cloudové prostředí AWS poskytuje vysokou úroveň bezpečnosti a komplexní zajištění vysoké dostupnosti díky provozu v clusteru a vysoké schopnosti zálohy a obnovy díky provozu napříč různými lokalitami v rámci prostoru EU.

Datová centra a služby AWS společnosti Amazon.com jsou provozována s klasifikací Tier III+, tak jak je definováno ve standardu TIA 942. Bližší informace je možné nalézt zde - https://aws.amazon.com/compliance/uptimeinstitute/.

5.1.2 Fyzický přístup

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.3 Elektřina a klimatizace

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.4 Vlivy vody

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.5 Protipožární opatření a ochrana

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.6 Ukládání médií

Všechna datová media jsou uložena v prostorách se stejným stupněm fyzického zabezpečení, jaký má prostor primárního pracoviště (Amazon.com AWS). Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno primární pracoviště.

Papírová média, která je nutno archivovat, jsou skladována v prostředí Poskytovatele, které se liší od primárního pracoviště

5.1.7 Zálohy

Zálohy technologie Služby jsou zajišťovány v rámci prostředí AWS splňujícím TIER III.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pracovní náplně v rámci správy Služby jsou přiděleny několika odděleným důvěryhodným rolím. Rozdělení funkcí mezi tyto důvěryhodné role vychází z požadavku oddělení jednotlivých oblastí činnosti, s omezením možnosti zneužití pravomocí.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Počty zaměstnanců na jednotlivých pozicích odpovídají potřebné míře oddělení odpovědností a zástupnosti a jsou detailně specifikovány v související interní dokumentaci. Činnosti související se Službou nevyžadují, aby byly vykonávány za účasti více než jedné osoby.

5.2.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům Služby identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke kterým má přístup. V systémech Služby je používaná identifikace jménem, resp. certifikátem, a autentizace heslem, resp. soukromým klíčem či jiná forma vícefaktorové autentizace.

5.2.4 Role vyžadující rozdělení povinností

Model rolí pro správu a provoz Služby je nastaven tak, aby nedocházelo ke kumulaci pravomocí. Role vyžadující rozdělení povinností jsou popsány v interní dokumentaci.

5.3 Personální bezpečnost

Do rolí spojených se správou a provozem Služby mohou být jmenováni pouze zaměstnanci Poskytovatele.

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

U každého pracovníka, který bude zařazen do role správy nebo dohledu Služby musí být zkoumána jeho způsobilost pro vykonávání povinností vyplývajících z této role.

5.3.2 Posouzení způsobilosti osob

Před obsazením pracovníka do klíčové role správy Služby musí být posouzena jeho způsobilost. Zdrojem informací pro toto posouzení není jen samotný pracovník, ale – a to zejména – osoby, se kterými pracoval a jeho nadřízení. Dalším neméně důležitým zdrojem jsou veřejně přístupné informační zdroje.

V rámci posuzování vhodnosti pracovníka pro konkrétní roli může být i požadavek na prokázání bezúhonnosti. Ta je posuzována podle výpisu z rejstříku trestů. V souladu se zavedenými postupy pro nábor zaměstnanců každý pracovník poskytuje tyto informace v průběhu vstupního osobního pohovoru. Pro doplnění informací, jejich ověření a aktualizaci mohou být prováděny další pohovory s odpovědnými pracovníky Poskytovatele.

Pracovníci, kteří jsou jmenováni do rolí bezpečnostních správců Služby smějí být vybíráni výhradně z vysoce spolehlivých a důvěryhodných zaměstnanců Poskytovatele.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci, podílející se na provozu, správě, údržbě a rozvoji Služby, jsou vyškoleni. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích. O provedení školení musí být proveden písemný zápis. U určených rolí může být školení nahrazeno prokazatelným seznámením pracovníka se všemi dokumenty upravujícími provoz Služby se vztahem k příslušné roli. Požadavky pro každou roli jsou stanoveny v interních směrnicích pro provoz Služby.

5.3.4 Požadavky a periodicita školení

V souvislosti s implementací nových vlastností a modelů provozu Služby musí pracovníci v rolích správy projít školením, kde jsou seznámeni s těmito novými vlastnostmi. Dále jsou povinni v rámci přidělené role udržovat a zvyšovat svoji kvalifikaci. Pravidelná školení pracovníků probíhají minimálně jednou za 12 měsíců.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Výměny osob mezi jednotlivými rolemi (přestupy z role do role) nejsou prováděny, ale je podporováno získávání znalostí pro výkon různých důvěryhodných rolí z důvodů zastupitelnosti a pro případ krizových situací.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Všechny neautorizované operace provedené pracovníky v rolích správy jsou považovány za hrubé porušení pracovní kázně a bezpečnostní incident. Jsou řešeny odpovídajícím způsobem.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Služba a technologie Služby nevyužívá nezávislé zhotovitele (dodavatele) s výjimkou samotné cloudové platformy AWS společnosti Amazon.com.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci Poskytovatele mají k dispozici, kromě této Politiky Služby, bezpečnostní a provozní dokumentace, veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti v rámci přidělených rolí.

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

Systém Služby zaznamenává informace o všech operacích provedených správci, informace o stavu a provozu systému Služby a o periodicky prováděných automatických operacích. Zaznamenávány jsou dále veškeré události požadované platnou legislativou.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

Auditní logy jsou zpracovávány při podezření, nebo po bezpečnostním incidentu. Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem a podléhají interní a externí kontrole.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu deseti let, pokud jiný předpis nestanoví dobu delší.

5.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy tak, aby byly ochráněny proti krádeži, modifikaci a zničení úmyslnému i neúmyslnému (ohněm, vodou) a vždy obsahují časový údaj o vzniku záznamu. Vybrané záznamy mohou být před změnou zabezpečeny elektronickou pečetí.

Auditní záznamy v podobě datových souborů jsou zabezpečeny a archivovány jako ostatní zálohy Služby – viz 5.1.6 a 5.1.7 .

5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy v písemné podobě nejsou obecně zálohovány; jsou pouze archivovány.

Auditní záznamy v elektronické podobě jsou zálohovány jako standardní součást záloh Služby včetně umístění záloh v jiné geografické lokalitě než primární prostředí.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Auditní záznamy jsou interně shromažďovány v rámci jednotlivých částí systému Služby dle interních pravidel.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Informace tohoto typu nejsou subjektům poskytovány.

5.4.8 Hodnocení zranitelnosti

Všechna závažná porušení bezpečnosti jsou okamžitě eskalována odpovědné osobě, nebo organizační složce.

5.5 Uchovávání informací a dokumentace

Použité mechanismy a procesní opatření jsou obecně předmětem interních předpisů upravujících problematiku dokumentace.

5.5.1 Typy informací a dokumentace, které se uchovávají

V rámci provozu Služby jsou archivovány informace pro účely auditu, výsledky provedených auditů, dokumentace registračního procesu a programového vybavení; data výsledků validačního procesu včetně všech podkladových dat a související smluvní dokumenty pro přístup ke Službě.

Dokumenty poskytnuté Službě k provedení ověření platnosti elektronických podpisů a pečetí nejsou uchovávány.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Programové vybavení, data, auditní záznamy a dokumenty se archivují po dobu deseti let.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Data a dokumenty v archivu jsou chráněny způsobem odpovídajícím jejich bezpečnostní citlivosti a významu. Mechanismy a procesní opatření jsou předmětem interních předpisů upravujících problematiku archivů.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací postupy jsou upraveny interní směrnicí a další relevantní interní dokumentací Poskytovatele.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Pokud jsou v rámci Služby využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka vydaná zvoleným QTSP.

5.5.6 Postupy pro získání a ověření uchovávaných informací a dokumentace

Správce Služby ověřuje neporušenost a celistvost archivu nejméně jednou ročně v rámci pravidelného interního auditu. Přístup k archivu má pouze Správce Služby a členové nezávislého týmu auditorů určeného Poskytovatelem podle pravidel popsaných v interní dokumentaci.

Správce Služby může určit pověřeného pracovníka Dohledu, aby průběžně prováděl kontrolu archivu.

5.6 Obnova po havárii nebo kompromitaci

5.6.1 Postup v případě incidentu a kompromitace

Postupy a chování v případě bezpečnostního incidentu nebo havárie jsou upraveny v dokumentu Havarijní plány a plán obnovy.

5.6.2 Poškození výpočetních prostředků, softwaru nebo dat

V případě poškození kterékoli z komponent, na kterých je poskytována Služba, se postupuje dle scénářů uvedených v dokumentu Havarijní plány a plán obnovy.

5.6.3 Schopnost obnovit činnost po havárii

Pokračování procesů Služby po havárii závisí na typu havárie a jejích následcích. Postupy pro zotavení po havárii jsou uvedeny v dokumentu havarijní plán a plán obnovy.

5.7 Ukončení činnosti CA nebo RA

Pro ukončování činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru platí následující pravidla:

- ukončení činnosti kvalifikovaného poskytovatele služby vytvářející důvěru musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu na využívání Kvalifikované služby OBELISK Validator QTS.
- ukončení činnosti poskytovatele služby vytvářející důvěru musí být zveřejněno na internetové adrese podle kapitoly 2.2 ,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb.

Poskytovatel se zavazuje poskytovat Službu 6 měsíců ode dne oznámení o ukončení činnosti.

verze 1.1 - PUBLIC

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle platné legislativy:

- informace o odnětí statutu musí být písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu na využívání Služby,
- informace o odnětí statutu musí být zveřejněna v souladu s kapitolou 2.2 ,
- o dalším postupu rozhodne ředitel společnosti SEFIRA na základě rozhodnutí orgánu dohledu.

6. TECHNICKÁ BEZPEČNOST

V této kapitole jsou definovány bezpečnostní požadavky na jednotlivé oblasti pro zajištění kvality poskytované Služby podle této Politiky.

6.1 Počítačová bezpečnost

6.1.1 Specifické technické požadavky na počítačovou bezpečnost

Jsou definovány v rámci interních směrnic pro provoz a řídí se těmito principy:

- Kritické systémy jsou umístěny ve fyzicky chráněném prostředí s řízeným přístupem.
- Kritické systémy jsou umístěny v Cloudovém prostředí s vysokou mírou zabezpečení s řízeným přístupem a odpovídající certifikací (Tier III a podobně)
- Na těchto počítačích jsou spuštěny nebo instalovány pouze programy související s provozem kritického systému.
- Provoz systémů je monitorován a pravidelně auditován.
- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.

6.1.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti Služby je založeno na požadavcích uvedených v mezinárodních a národních standardech, zejména:

- ETSI EN 319 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 403 – Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers
- ETSI TS 119 101 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
- ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- ETSI TS 103 171 – Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile
- ETSI EN 319 132 - Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures
- ETSI TS 103 172 – Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile
- ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures
- ETSI TS 103 173 – Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile
- ETSI EN 319 122 - Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures
- ETSI TS 103 174 – Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile
- ETSI EN 319 162 - Electronic Signatures and Infrastructures (ESI); ASiC

6.2 Bezpečnost životního cyklu

6.2.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací a best practice postupy pro vývoj software.

6.2.2 Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity a kontrolami bezpečnostní shody.

6.2.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v SEFIRA prováděno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz – účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování – zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování – provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.3 Síťová bezpečnost

Zabezpečení sítí je popsáno v interních směrnicích pro provoz. Je kladen maximální důraz na důkladné zabezpečení všech komponent:

- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.
- Počítačové sítě kritických systémů Poskytovatele jsou odděleny od běžné podnikové sítě pomocí interního firewallu.
- Provoz systémů je monitorován a pravidelně auditován.
- Kontroly a ověřování průchodnosti sítě jsou pravidelně prováděny prostřednictvím technických správců v rámci Poskytovatele.

7. HODNOCENÍ SHODY A JINÁ HODNOCENÍ

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Pro zajištění definované úrovně bezpečnosti infrastruktury a tím i vysoké kvality poskytovaných služeb, je prováděna pravidelná kontrola shody. Tato kontrola je prováděna minimálně jednou za 12 měsíců formou bezpečnostního auditu.

Další pravidelné audity dané nařízením eIDAS a prováděné k tomu určeným, akreditovaným posuzovatelem shody jsou prováděny vždy v intervalu kratším než 24 měsíců.

Při každé změně HW a SW vybavení, na kterém jsou Služby poskytovány, musí být zkoumán dopad změn na bezpečnost a kvalitu služeb.

Všechny tyto pravidelné audity a kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí bezpečnostního ředitele SEFIRA, případně i vedení SEFIRA.

O provedení každé kontroly musí být vypracována podepsaná písemná zpráva. Zpráva je archivována stejným způsobem jako ostatní záznamy o provozu Služby a uchovávána nejméně po dobu deseti let.

7.2 Identita a kvalifikace hodnotitele

Kvalifikace externího auditora provádějícího hodnocení podle nařízení eIDAS je dána požadavky tohoto nařízení.

7.3 Vztah hodnotitele k hodnocenému subjektu

Pravidelná kontrola provozu je prováděna interními pracovníky SEFIRA.

V případě externího hodnotitele platí, že se jedná o subjekt, který není se SEFIRA majetkově ani organizačně svázán.

7.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného nařízením eIDAS jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány standardy, podle kterých je hodnocení prováděno.

7.5 Postup v případě zjištění nedostatků

Všechny zjištěné nedostatky jsou komunikovány v rámci auditní zprávy. Podle charakteru nedostatku jsou naplánovány a provedeny činnosti technologického (konfigurační změny, implementace dalších technologických opatření atd.) charakteru a/nebo doplněna a aktualizována relevantní dokumentace tak, aby byl nedostatek odstraněn.

7.6 Sdělování výsledků hodnocení

Všechny skutečnosti zjištěné vyhodnocením informací získaných auditem jsou formou auditní správy prezentována vedení SEFIRA, které přijme konkrétní opatření vyplývající ze zjištění auditu. S výsledkem je seznámen také Bezpečnostní ředitel SEFIRA. Sdělování výsledků hodnocení podléhá požadavkům legislativy.

8. OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

Poskytování Služby je zpoplatněno dle ceníku Poskytovatele.

8.2 Citlivost obchodních informací

8.2.1 Výčet citlivých informací

Za důvěrné jsou považovány následující informace:

- veškeré informace týkající se procesu ověření a uložené v rámci Služby včetně auditních záznamů,
- veškeré soukromé klíče používané v rámci jednotlivých procesů Služby,
- obchodní informace Poskytovatele,
- veškeré informace a dokumentace s ohledem na poskytování služeb vytvářejících důvěru,
- výsledky interních a externích auditů Služby,
- veškeré osobní údaje.

Nakládání s těmito informacemi je limitováno. Smějí být zveřejněny pouze v souladu s touto politikou, nebo zákonnými normami České republiky. Důvěrné informace jsou chráněny technickými a administrativními prostředky a jejich zveřejnění mimo povolenou mez je považováno za hrubé porušení této politiky, případně dalších souvisejících předpisů.

8.2.2 Informace mimo rámec citlivých informací

Informace v certifikátech, seznamy zneplatněných certifikátů, důvod zneplatnění a další informace, které nejsou označeny jako důvěrné, obecně nejsou za důvěrné považovány a smějí být sděleny nebo zveřejněny.

8.2.3 Odpovědnost za ochranu citlivých informací

Zaměstnanec, který nakládá s údaji a informacemi uvedenými v kap. 8.2.1 Výčet citlivých informací je zodpovědný za jejich ochranu. Tyto informace nesmí být poskytnuty třetí straně bez souhlasu vlastníka Služby, nebo vedení SEFIRA.

8.3 Ochrana osobních údajů

SEFIRA zajišťuje ochranu osobních údajů osob, k nimž získá přístup při provozu Služby. Zásady ochrany osobních údajů jsou obsaženy v této Politice a vycházejí z obecně závazných právních předpisů České republiky, zejména nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu

těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – GDPR) a zákona č. 101/2000 Sb., o ochraně osobních údajů.

8.4 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systému poskytujícího Službu, jsou chráněny autorskými právy společnosti SEFIRA spol. s r.o., a představují její významné know-how a práva duševního vlastnictví.

8.5 Zřeknutí se záruk

QTSP a TSP SEFIRA odmítá jakékoliv záruky na provoz Služby a výsledky poskytnuté Službou, pokud byla Služba a/nebo Rozhraní použito v rozporu s podmínkami použití Služby a touto Politikou.

8.6 Omezení odpovědnosti

Společnost SEFIRA spol. s r.o. neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované touto Politikou, podle které byla Služba poskytována. Dále neodpovídá za škody vzniklé v důsledku porušení závazků SEFIRA z důvodu vyšší moci.

8.7 Odpovědnost za škodu, náhrada škody

Povinnost SEFIRA k náhradě škody či nemajetkové újmy touto obchodní společností způsobené nikoliv úmyslně, z hrubé nedbalosti či na přirozených právech člověka porušením jakýchkoliv jejích závazků a/nebo povinností v souvislosti s poskytování Uznávané služby je omezena částkou 100 000,- Kč (slovy: jedno sto tisíc korun českých), kterážto částka představuje ve smyslu ustanovení § 2898 zákona č. 89/2012 Sb., občanský zákoník, v platném znění maximální částku náhrady škody či nemajetkové újmy, za kterou odpovídá SEFIRA a kterou bude případně povinna uhradit.

Pokud je poskytována Uznávaná služba, je důkazní břemeno, pokud jde úmysl nebo nedbalost TSP, na fyzické či právnické osobě uplatňující nárok na náhradu škody podle druhé věty prvního odstavce Článku 13 nařízení eIDAS.

Pokud je poskytována Kvalifikovaná služba, je důkazní břemeno na straně QTSP a je jeho právem prokázat, že škoda podle třetí věty prvního odstavce Článku 13 nařízení eIDAS nastala bez jeho úmyslu nebo nedbalosti.

8.8 Doba platnosti, ukončení platnosti

8.8.1 Doba platnosti

Počátek platnosti tohoto dokumentu je určen dnem vydání uvedeným v kapitole 1.2 .

Konec platnosti tohoto dokumentu je určen dnem ukončení platnosti. Politika zůstává v platnosti do doby ukončení poskytování Služby nebo do okamžiku nahrazením novou Politikou. Aktualizace ustanovení Politiky nahrazují ustanovení neplatná.

8.8.2 Ukončení platnosti

Všechny aktualizace této Politiky, jakož i ukončení její platnosti schvaluje ředitel SEFIRA.

8.9 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může SEFIRA využít všechny typy kontaktů jako jsou dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat se SEFIRA lze taktéž způsoby uvedenými v kapitole 2.2 této Politiky.

8.10 Změny

8.10.1 Postup při změnách

SEFIRA je oprávněna v budoucnosti doplnit tuto Politiku o ustanovení, jejichž nutnost bude teprve zjištěna. Takové změny budou zveřejněny na místech definovaných v kapitole 2.2 této Politiky. Případné změny nebudou mít zpětnou platnost.

8.10.2 Postup při oznamování změn

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

8.10.3 Okolnosti, při kterých musí být změněn validační proces

Validační proces je dán několika technickými specifikacemi a normami definovanými v nařízení eIDAS. Validační proces se řídí těmito legislativními a technickými požadavky a jeho změna je možné pouze tak aby splnila požadavky legislativní.

8.11 Řešení sporů

Kterýkoliv spor, jež nelze řešit smírně, bude předmětem soudního rozhodnutí. Řešení veškerých sporů právního charakteru bude podstoupeno soudnímu rozhodnutí. Soudní jednání se bude konat na území České republiky v českém jazyce.

8.12 Rozhodné právo

Rozhodným právem pro řešení sporů je legislativa České republiky.

8.13 Shoda s právními předpisy

Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s legislativními požadavky EU, České republiky a dále s relevantními mezinárodními standardy – viz kapitola 6.1.2 této Politiky.