sefira

POLITIKA

Kvalifikovaná služba – OBELISK Remote Sign

Verze	1.0
Datum	15. 05. 2026
Autor	Petr Dolejší
Počet stran	41

SEFIRA spol. s r.o. | Antala Staška 2027/77 | 140 00 Praha 4 | +420 222 558 111 | sales@sefira.com | www.sefira.com

Upozornění

Tento veřejný dokument je určen pro potřebu společnosti SEFIRA spol. s r.o. a obsahuje politiku provozu kvalifikované služby **OBELISK Remote Sign** pro správu kvalifikovaných prostředků pro vytváření el. podpisů na dálku. 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.

Historie změn

Datum	Platnost od	Popis	Verze	Schválil
10.4.2026		Interní draft	0.1	
24.4.2026		doplnění onPrem zákaznické varianty	0.2	
15.5.2026	21.5.2026	Finální schválená verze	1.0	Řídící orgán

Obsah

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 kvalifikované služby pro správu kvalifikovaných prostředků pro vytváření el. podpisů na dálku **OBELISK** Remote Sign (dále jen „OBELISK Remote Sign“ nebo „Kvalifikovaná služba“).

Kvalifikovaná služba provozovaná společností SEFIRA spol. s r.o. jako kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dále též obecně jako „Služba“), zajišťující vytváření el. podpisů na dálku prostřednictvím kvalifikovaných prostředků koncovým uživatelům a spoléhajícím se stranám (dále jen „Klient“) je poskytována všem Klientům na základě uzavřeného smluvního vztahu (dále jen „Smlouva“).

Služba je provozována ve dvou režimech:

- centrální služba kvalifikovaných prostředků Poskytovatele v datovém centru pod správou Poskytovatele s klientskou aplikací RSE hostovanou u Klienta, dále jako Centrální služba a
- provoz kvalifikovaného prostředku včetně klientské aplikace RSE nasazených v prostředí Klienta pod správou Poskytovatele, dále jako Hostovaná služba.

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 a to především:

- právní úprava týkající se elektronického podpisu a pečeti v souladu s nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění a
- zákon České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

1.2. Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Politika kvalifikované služby správy kvalifikovaných prostředků pro vytváření el. podpisů na dálku, verze 1.0 - PUBLIC
OID politiky:	není přiděleno
Datum vydání:	21. května 2026
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 kvalifikovaný poskytovatel služeb vytvářejících důvěru pro Kvalifikovanou službu **OBELISK Remote Sign**.

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, dále také jako Klient.

V případě Klientů využívajících Hostovanou službu, jsou HW a SW prostředky Hostované služby umístěny v datových centrech Klienta.

1.3.3. České Radiokomunikace a.s. (ČRa)

ČRa je poskytovatel geograficky oddělených datových center umístěných v ČR ve kterých jsou fyzicky hostovány HW a SW prostředky Centrální služby. 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 správu kvalifikovaných prostředků pro vytváření el. podpisů na dálku.

Službu je možné čerpat pouze prostřednictvím definovaných Rozhraní, která jsou Klientovi Poskytovatelem zpřístupněny.

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
autentizační certifikát	v tomto dokumentu certifikát sloužící pro autentizaci přístupu ke Službě
Centrální služba	Služba v režimu centrální služby kvalifikovaných prostředků Poskytovatele v datovém centru pod správou Poskytovatele
certifikát	v tomto dokumentu kvalifikovaný certifikát pro elektronické podpisy nebo pečetě
ČSN	označení českých technických norem
DTBS	Data to be Signed – principiálně hash podepisovaných nebo pečetěných dat
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
HSM	Hardware Security Module
Hostovaná služba	Služba v režimu provozu kvalifikovaného prostředku nasazeného v prostředí Klienta pod správou Poskytovatele
IS	informační systém
Klient	Spoléhající se strana

Klientská aplikace	Aplikační řešení tvořící Rozhraní Služby založené na technologii Remote Signing Engine
Kvalifikovaná služba	Kvalifikovaná služba správy kvalifikovaných prostředků pro vytváření el. podpisů na dálku je kvalifikovaná služba vytvářející důvěru vytvořená a provozovaná kvalifikovaným poskytovatelem vytvářejícím důvěru SEFIRA
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 Remote Sign	Označení Služby správy kvalifikovaných prostředků pro vytváření el. podpisů na dálku
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
Politika	tento dokument politiky provozu Služby pro správu kvalifikovaných prostředků pro vytváření el. podpisů na dálku
Poskytovatel	Poskytovatel Služby správy kvalifikovaných prostředků pro vytváření el. podpisů na dálku, společnost SEFIRA spol. s r.o.
QSCD	Qualified Signature/Seal Creation Device – kvalifikovaný prostředek pro vytváření el. podpisů a pečetí
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, primárně ve formě řešení RSE pro vytváření el. podpisů na dálku.
rQSCD	Obecné označení pro kvalifikovanou službu vytvářející důvěru pro správu kvalifikovaných prostředků pro vytváření el. podpisů a pečetí na dálku poskytovaná kvalifikovaným poskytovatelem služeb vytvářejících důvěru SEFIRA bez ohledu na její variantu
RSE	Řešení Remote Signing Engine, dále také jako Klientská aplikace nebo Rozhraní
SAM	Signature Activation Module – primární certifikovaná technologie plní roli kvalifikovaného prostředku pro vytváření el. podpisů/pečetí (QSCD)
SEFIRA	Společnost SEFIRA spol. s r.o. jako Poskytovatel, TSP nebo QTSP
Služba	obecné označení pro poskytovanou službu správy kvalifikovaných prostředků pro vytváření el. podpisů na dálku není-li rozhodující dotčená její varianta – Centrální služba nebo Hostovaná 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 využívající při své činnosti služby kvalifikovaných prostředků pro vytváření el. podpisů a pečetí na dálku
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
veřejný klíč	souhrnné označení dat pro ověřování elektronického podpisu či pečeti 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.

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

SEFIRA poskytuje Službu jako QTSP po zveřejnění na příslušném TL v režimu Kvalifikované služby. 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 https://sefira.com.

Elektronická adresa, která slouží pro kontakt veřejnosti se SEFIRA, je info@sefira.com. ID datové schránky společnosti SEFIRA je ts8zphg.

Na internetové adrese https://sefira.com/qts/ lze získat informace o Službě.

Elektronická adresa pro hlášení požadavků a neshod ze strany Klienta je support@sefira.com. Tato adresa je součástí service desk řešení používaného společností SEFIRA pro komunikaci s uživateli Služby.

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 (Digitální a informační agentura) 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.

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

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

Každý uživatel, který je do Služby registrován musí být vždy ztotožněn jak pro účely samotného zřízení přístupu ke Službě, respektive do Klientské aplikace, tak v případě párování přiděleného vícefaktorového prostředku tak i při samotném procesu vydávání kvalifikovaného certifikátu ze strany příslušné registrační autority.

Rozsah osob oprávněných pro získání přístupu ke Službě je uveden ve Smlouvě. Tyto oprávněné osoby mohou požádat o přidělení nezbytných autentizačních údajů pro přístup ke Službě.

3.1.2. Registrace IS jako klienta Služby

Osoby zastupující Klienta pro správu řízení přístupu ke Službě jsou uvedeny ve Smlouvě. Tyto zastupující osoby mohou požádat o přidělení autentizačních údajů pro přístup vlastních IS ke Službě prostřednictvím jejího Rozhraní.

3.2. Autentizace ke Službě

Autentizace přístupu uživatele nebo IS ke Službě je možná pouze prostřednictvím Rozhraní pomocí přidělených autentizačních údajů. Autentizačními údaji pro informační systémy napojené na Službu prostřednictvím Rozhraní mohou být autentizační certifikáty vydané Poskytovatelem Služby. Autentizačními údaji pro koncově uživatele jsou typicky vícefaktorové autentizační mechanismy sestávající se primárně z kombinace uživatelské jméno a heslo a samostatného druhého faktoru typicky ve formě mobilní aplikace.

3.3. Ukončení čerpání Služby

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

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

3.4. Rušení uživatelských účtů

Rušení přístupových účtů ke Službě se provádí:

- u běžných uživatelů na základě postupů Klienta spočívajících v ukončení oprávnění pro daného uživatele;
- na základě písemné žádosti oprávněné osoby uvedené ve Smlouvě;
- automaticky v případě ukončení Smlouvy.

4. Požadavky na životní cyklus Služby OBELISK Remote Sign

Služba zpracovává na svém vstupu celé dokumenty nebo pouze reprezentaci dokumentů (DTBS), které mají být podepsány prostřednictvím kvalifikovaných prostředků, jejichž správa je předmětem Služby dle 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 ve znění pozdějších předpisů 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

Tato Služba je Poskytovatelem vytvořena za účelem umožnění provozu řešení umožňujících vytváření kvalifikovaných elektronických podpisů na dálku. Za tímto účelem Poskytovatel vybudoval komplexní řešení, které zajišťuje provoz certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí (QSCD) tak, aby připojené obslužné aplikace mohly na straně jedné prostřednictvím Rozhraní tyto QSCD prostředky využívat a zároveň byl provoz QSCD prostředků zajištěn v souladu s příslušnými certifikaci a standardy pod výhradní kontrolou Poskytovatele, aby bylo možné do těchto QSCD prostředků vydávat kvalifikované certifikáty pro elektronický podpis s příslušnými atributy qc_statements a výsledné elektronické podpisy byly považovány za kvalifikované elektronické podpisy dle nařízení eIDAS.

Služba podporuje následující algoritmy a formy podpisu:

- RSA-PSS, délka klíče 2048, 3072 a 4096 bitů
- RSA-PKCS1, délka klíče 2048, 3072 a 4096 bitů
- ECDSA, ve variantách secp256r1, prime256v1, secp384r1, prime384v1, secp521r1, prime521v1
- Hashovací algoritmy SHA-256, SHA-384 a SHA-512

Výše uvedené algoritmy jsou podporovány bez ohledu na požadovaný výsledný formát el. podpisu. Výsledný formát, resp. formát dat, které je možné podepsat je v odpovědnosti Klientské aplikace napojené na kvalifikované prostředky Službu.

Klientská aplikace Služby podporuje následující datové formáty podpisů:

- PAdES (PDF)
- XAdES (XML)
- PKCS#1 (pro DTBS)

V případě využití možnosti podpisu pouze DTBS vytváří Služba samotný objekt podpisu, který může aplikace volající Rozhraní Služby využít pro libovolný jí podporovaný výstupní formát.

4.2.1. Základní architektura

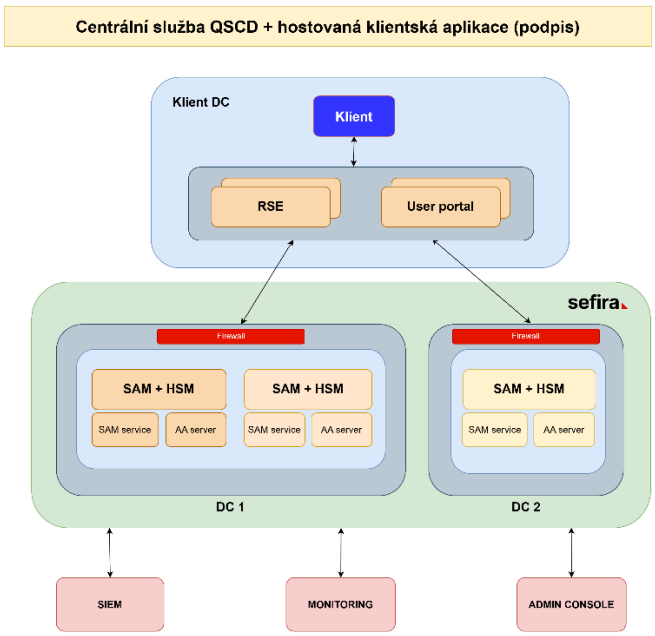
Základní architekturu služby tvoří certifikované Signature/Seal Activation Moduly (SAM) a k němu příslušný kryptografický Hardware Security Modul (HSM) v souladu s certifikací zajišťující bezpečnou správu klíčů a certifikátů. A dále řešení Rozhraní implementované Klientskou aplikací RSE.

Bez ohledu na režim Služby jsou vždy využívány stejná technologická řešení certifikovaných SAM modulů a odpovídajících certifikovaných kryptografických prostředků. Správa kvalifikovaných prostředků je vždy výhradní ze strany Poskytovatele.

Centrální služba

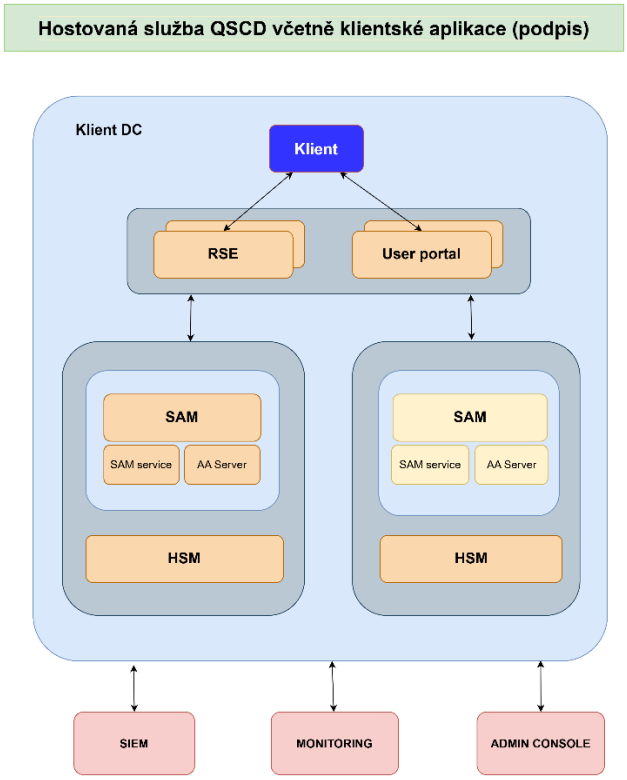
Centrální služba disponuje několika SAM moduly provozovanými napříč minimálně 2 geograficky oddělenými datovými centry z důvodů zajištění vysoké dostupnosti a odolnosti služby. Služba je připravena využívat různé formy a verze certifikovaných podpůrných kryptografických prostředků.

Odpovídající Rozhraní ve formě Klientské aplikace je implementováno v prostředí infrastruktury Klienta.



Hostovaná služba

V případě Hostované služby jsou jednotlivé SAM moduly spolu se sdílenými kryptografickými prostředky provozovány v prostředí Klienta v takovém režimu dostupnosti, jak odpovídá potřebám konkrétního klienta.



4.2.2. Způsob využívání Služby

Hranicí Služby je Rozhraní řešení RSE v hostované podobě, která umí kvalifikované prostředky využít, a které je se Službou přímo integrováno.

Předpokladem pro plnohodnotné využívání Služby je zajištění dodatečných služeb kvalifikovaného poskytovatele služeb vytvářejících důvěru poskytujících služby vydávání kvalifikovaných certifikátů pro el. podpisy. Tyto služby Poskytovatel Klientům umožňuje přímo zprostředkovat v roli registrační autority a na základě přímé integrace Rozhraní na aplikační rozhraní Poskytovatele minimálně v rozsahu předávání žádostí o vydání/obnovu certifikátů a získání vystavených certifikátů pro uživatele za účelem jejich registrace a aktivace v rámci Služby.

4.3. Zřízení Služby

Zřízení Služby probíhá na základě uzavřené Smlouvy o poskytování Služby mezi Poskytovatelem a Klientem. Tato Smlouva musí být uzavřena v písemné formě a podepsána:

- klasicky vlastnoručním podpisem na papírový dokument, nebo

- bezpapírově/elektronicky pomocí osobního kvalifikovaného certifikátu osoby zastupující Klienta.

Osoba zastupující Klienta je povinna zejména:

- seznámit se s touto Politikou a s Certifikační politikou vydávání kvalifikovaných certifikátů pro elektronické podpisy na dálku zvoleného poskytovatele a smluvně se zavázat jednat podle nich,
- seznámit se se Smlouvou,
- dodržovat veškerá ustanovení Smlouvy,
- používat Službu v souladu s ustanoveními kapitoly 1.4,
- nakládat s údaji pro identifikaci a autentizaci ke Službě tak, aby nemohlo dojít k jejímu zneužití,
- neprodleně vyrozumět Poskytovatele Služby o podezření, že údaje pro identifikaci a autentizaci ke Službě byly zneužity a požádat o zneplatnění Certifikátů,
- neprodleně uvědomit Poskytovatele Služby o změnách údajů uvedených ve Smlouvě,
- poskytovat pravdivé a úplné informace pro zřízení Služby,
- překontrolovat, zda údaje získané z předložených dokumentů jsou správné a odpovídají požadovaným údajům,
- v případě požadavku na ukončení Služby je povinností Osoby informovat o této skutečnosti Poskytovatele a po vzájemné dohodě sjednanou formou Smlouvu ukončit.

Poskytovatel Služby je povinen zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované platnou právní úpravou a technickými standardy,
- v procesu zřizování Služby ověřit všechny ověřitelné údaje podle předložených dokladů,
- zprostředkovat vydání Certifikátu obsahujícího věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto Certifikátu a v souladu s postupy zvoleného kvalifikovaného poskytovatele vydávajícího certifikáty,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- činnosti spojené se Službou poskytovat v souladu s platnou právní úpravou, touto Politikou, bezpečnostní politikou a s provozní dokumentací.

4.4. Aktivace Služby

Pro aktivaci Služby, resp. spravovaných QSCD prostředků, pro potřeby podepisování, je v rámci procesu aktivace Služby zajištěno především:

- vydání autorizačních údajů pro přístup ke Službě,
- registrace oprávněných aplikací Klienta využívající Službu (v hostované podobě),
- zpřístupnění aplikace uživatelského portálu pro řešení RSE Klientovi v rámci jeho Klientské aplikace pro umožnění individuální správy klíčů a certifikátů koncovými uživateli s využitím registrovaných vícefaktorových prostředků.
- zprostředkování vydání Certifikátů od podporovaného kvalifikovaného poskytovatele a
- registrace Certifikátů prostřednictvím jejího Rozhraní.

4.5. Používání Služby

Pro zajištění plnohodnotné funkčnosti vytváření podpisů na dálku obsahuje Služba klientskou aplikaci RSE plně kompatibilní s použitými QSCD. Klientská aplikace je vždy provozována v hostované podobě a je třeba zajistit dostatečné zdroje pro její implementace a provoz.

4.6. Dostupnost Služby

4.6.1. Centrální služba

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 službami datových center v rámci kterých je Služba provozována.

Poskytovatelem garantovaná minimální dostupnost je uvedena ve Smlouvě. Celková garantovaná dostupnost je ovlivněna podmínkami provozu datových center Klienta, ve kterých je provozována Klientská aplikace RSE.

4.6.2. Hostovaná služba

V případě Hostované služby je Služba provozována v režimu vysoké dostupnosti s minimálně 2 aktivními uzly.

Celková garantovaná dostupnost je určena podmínkami provozu datových center Klienta, ve kterých je Služba a její součásti provozována.

4.7. Úschova dat o provedených transakcích prostřednictvím Služby

Doba, po kterou jsou uchovávány záznamy potřebné pro prokázání vytváření klíčů, generování certifikátů a provedení transakcí prostřednictvím Služby, činí minimálně 10 let.

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 jsou umístěny v datových centrech poskytujících vysokou úroveň bezpečnosti nejenom fyzické, ale též provozní (chlazení, dodávky energií, konektivity). Vysoká dostupnost Služby je zajištěna díky provozu více identických zařízení v clusteru v různých geograficky oddělených datových centrech napříč různými lokalitami v rámci prostoru EU.

Používaná datová centra společnosti České Radiokomunikace jsou provozována s klasifikací Tier III. Bližší informace je možné nalézt zde – https://www.cra.cz/ict-reseni/datova-centra.

5.1.2. Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci Poskytovatele.

Ochrana objektů datových center je řešena elektronickým zabezpečovacím systémem (EZS) s dohledem provozovatele 24/7.

5.1.3. Elektřina a klimatizace

V prostorách určených k provozu Služby je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20 °C ± 5 °C. Přívod elektrické energie je jištěn pomocí více zdrojů el. energie, UPS a/nebo záložních diesel agregátů.

5.1.4. Vlivy vody

Všechny kritické systémy nezbytné pro provoz Služby jsou umístěny v datových centrech mimo záplavové oblasti. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5. Protipožární opatření a ochrana

V datových centrech pro provoz Služby objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Prostředí pro provoz Služby jsou vybavena systémem pro hašení požárů.

5.1.6. Ukládání médií

Všechna datová media jsou uložena v prostorách se stejným stupněm fyzického zabezpečení, jaký má prostor provozu Služby. Kopie záznamů jsou ukládány v jiné geografické lokalitě, než kde je Služba provozována.

Papírová média, která je nutno archivovat, jsou skladována v prostředí Poskytovatele, které se liší od místa provozu Služby.

5.1.7. Zálohy

Zálohy technologie Služby jsou zajišťovány prostřednictvím náhradních fyzických zařízení v několika datových centrech typu TIER III. Zálohy logů, SW a konfigurace nezbytných pro obnovu fyzických zařízení v případě jejich poruchy jsou ukládány mimo prostor provozu Služby na minimálně 2 místech, s tím, že jedním místem je sídlo Poskytovatele.

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.

Pro vybrané činnosti související se Službou je vyžadována účast více než jedné osoby. Jedná se především o:

- inicializaci Služby (především její kryptografické prostředky – SAM, HSM) pro generování a ukládání citlivých dat nutných pro provoz Služby,
- změna konfigurace kryptografických prostředků,
- obnova Služby a jejích kryptografických prostředků.

Pro ostatní činnosti se nevyžaduje, aby byly vykonávány za účasti více než jedné osoby, ale vždy se musí jednat o pověřené pracovníky Poskytovatele.

5.2.3. Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu ke kvalifikovaným 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.

Pro správu kryptografických prostředků je využíváno principu systém více očí ve spojení s HW prostředky vícefaktorové autorizace.

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 poskytovatelů služeb datových a cloudových center ve kterých je Služba provozována (Centrální služba) a/nebo Klienta zajišťujícího provoz datových center pro Hostovanou službu.

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. Záznamy jsou zároveň ukládány v centrálním log managementu a SIEM řešení Poskytovatele.

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.

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. Zároveň jsou tyto záznam replikovány do centrálního logovacího řešení Poskytovatele v cloudu v rámci EU se samostatným zálohováním a řízením dostupnosti těchto záznamů.

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

Hodnocení zranitelnosti je Poskytovatelem prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících s provozem Služby je popsáno v interní dokumentaci. Všechna závažná porušení bezpečnosti jsou 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 o vytvoření/smazání klíčů, data o využití klíčů konkrétním Klientem včetně všech podkladových dat a související smluvní dokumenty pro přístup ke Službě.

Data předávaná Službě k podepisování, tedy celé dokumenty nebo pouze DTBS, nejsou ukládána.

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 plány a plán obnovy.

5.7. Ukončení činnosti

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 Remote Sign.
- 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.

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. Kryptografie, soukromý klíč a jeho ochrana

V rámci Služby je využíváno algoritmů RSA a ECDSA. Délka klíčů odpovídá aktuálním požadavkům ETSI TS 119 312. Klíčové páry klientů Služby jsou generovány a soukromé klíče jsou zabezpečeny prostřednictvím SAM modulu a kryptografického HSM modulu v režimu zařízení typu QSCD pod výhradní kontrolou Poskytovatele. Přístup k soukromým klíčům je chráněn kryptografickým protokolem, který zajišťuje, že klíč může použít pouze jeho oprávněný držitel (organizace nebo uživatel). Soukromé klíče klientů jsou ukládány a zálohovány v zašifrované podobě v prostředí klientské aplikace využívající Službu, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení a tyto klíče není možné využít jinak než prostřednictvím kvalifikovaných prostředků Služby.

6.2. Počítačová bezpečnost

6.2.1. 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 datovém centru s vysokou mírou zabezpečení s řízeným přístupem a odpovídající certifikací (Tier III a podobně)
- Na těchto systémech jsou spuštěny nebo instalovány pouze programy související s provozem Služby, dohledem nad ní a zálohováním.
- Provoz systémů je monitorován a pravidelně auditován.
- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.

6.2.2. Hodnocení počítačové bezpečnosti

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

- ČSN EN 419241-1 Důvěryhodné systémy podporující podpisový server – Část 1: Obecné bezpečnostní požadavky systému.
- EN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements.
- ČSN EN 419241-2 Důvěryhodné systémy podporující podpisový server – Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis.

- EN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- ČSN EN 419221-5 – Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografické modul pro důvěryhodné služby.
- EN 419221-5 – Protection Profiles for TSP Cryptographic Modules – Part 5 - Cryptographic Module for Trust Services.
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.
- ETSI TS 119 432 Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation.
- 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

6.3. Bezpečnost životního cyklu

6.3.1. Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací a best practice postupy pro vývoj software a zároveň jsou používány pouze komponenty certifikované a uvedené na příslušných seznamech Evropské unie jako QSCD.

6.3.2. Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity a kontrolami bezpečnostní shody a řídí se těmito normami:

- ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky.
- ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti.
- ČSN EN ISO/IEC 27017 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002.
- ČSN EN ISO/IEC 27018 informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII.

6.3.3. 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 v souladu s normami ČSN EN ISO 9001 a ČSN EN ISO/IEC 27001:

- 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.

6.4. 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 samostatného firewallu.
- Provoz systémů je monitorován a pravidelně auditován.
- Kontroly a ověřování průchodnosti sítě jsou pravidelně prováděny prostřednictvím technických správců Poskytovatele.
- Veškerá komunikace mezi Klientskými aplikacemi a Službou je vedena šifrovaně. Podrobnosti jsou popsány v interní dokumentaci.

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 a rovněž v rámci pravidelných auditů ISMS.

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. Finanční odpovědnost

8.2.1. Krytí pojištěním

Poskytovatel prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční náhrady.

8.2.2. Další aktiva

Poskytovatel prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná finanční zajištění na poskytování služeb vytvářejících důvěru s ohledem na riziko vzniku odpovědnosti za škodu. Podrobné informace o aktivech Poskytovatele je možno získat z Výroční zprávy Poskytovatele uveřejněné v obchodním rejstříku.

8.3. Důvěrnost obchodních informací

8.3.1. Výčet důvěrných informací

Za důvěrné jsou považovány následující informace:

- veškeré informace týkající se nastavení a způsobu zpracování 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.

8.3.2. Informace mimo rámec důvěrných 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.

8.3.3. Odpovědnost za ochranu důvěrných informací

Zaměstnanec, který nakládá s údaji a informacemi uvedenými v kap. 8.3.1. Výčet důvěrných informací je zodpovědný za jejich ochranu. Tyto informace nesmí být poskytnuty třetí straně bez souhlasu vlastníka Služby, nebo vedení SEFIRA.

8.4. 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.

8.5. 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.

8.6. Zastupování a záruky

Poskytovatel zaručuje, že poskytuje:

- technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s provozem Služby prostřednictvím kontaktních údajů uvedených na adrese https://sefira.com/qts/ nebo v této Politice,
- Službu vždy právně a technicky aktuální dle relevantních právních předpisů a technických standardů a norem.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud Klient využívající Službu neporušil povinnosti plynoucí mu ze Smlouvy a této Politiky.

8.7. Zřeknutí se záruk

Poskytovatel 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.

8.8. 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.

8.9. Odpovědnost za škodu, náhrada škody

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platných právních předpisů a dále takové záruky, které byly sjednány Smlouvou mezi Poskytovatelem a Klientem Služby. Smlouva nesmí být v rozporu s platnou právní úpravou a musí být vždy v elektronické nebo listinné formě.

Poskytovatel:

- se zavazuje, že splní veškeré povinnosti definované jak platnými právními předpisy, tak příslušnými politikami a
- poskytuje výše uvedené záruky po celou dobu platnosti Smlouvy o poskytování Služby.

Poskytovatel neodpovídá za vady poskytnuté Služby vzniklé z důvodu nesprávného nebo neoprávněného využívání Služby poskytnutých v rámci plnění Smlouvy o poskytování Služby Klientem, zejména za využívání v rozporu s podmínkami uvedenými v této Politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení.

Reklamaci je možné podat těmito způsoby:

- e-mailem na adresu info@sefira.com,
- prostřednictvím datové schránky Poskytovatele,
- doporučenou poštovní zásilkou na adresu sídla Poskytovatele,
- osobně v sídle společnosti.

Reklamující osoba je povinna uvést:

- co nejvýstižnější popis závady,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne Poskytovatel nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, nebo doporučenou zásilkou), pokud se strany nedohodnou jinak. Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak. Další možné náhrady škody vycházejí z ustanovení příslušných právních předpisů a o jejich výši může rozhodnout soud.

8.10. Doba platnosti, ukončení platnosti

8.10.1. 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.

8.10.2. Ukončení platnosti

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

8.11. 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.

8.12. Změny

8.12.1. Postup při změnách

Poskytovatel je oprávněn 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.

8.12.2. Postup při oznamování změn

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

8.13. 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.

8.14. Rozhodné právo

Rozhodným právem pro řešení sporů je legislativa České republiky.

8.15. 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 6.2.2. této Politiky.