eIDAS SMART TRUST eLECTRONIC PLATFORM

ELDAx Q-validation

POLITIKA SLUŽBY

Označení dokumentu	**ELDAx Q-validation Politika služby**	**STÁDIUM:**	**Schváleno**
Release ELDAx	7.99	**DŮVĚRNOST:**	Veřejné
ZE DNE:	28. 4. 2022	**DATUM AKTUALIZACE:**	01. 06. 2026
ZPRACOVAL / AUTOR:	Ondřej Holub, Pavel Jedlička	**VERZE DOKUMENTU:**	1.2

Pojem	Definice
Služby	Služby platformy je soubor funkcionalit, který lze dosáhnou dosáhnout konfigurací licence na základě pořízení jednotlivých modulů platformy ELDAx.
Komponenty	Komponenty jsou základní stavební celky celé platformy. Komponenty jsou v současné době ELDAxPOTRAL a ELDAxSTORAGE. Komponenty je skládají z jednotlivých modulů. Moduly, kromě ELDAx/BASE, který je základní licencí, nemají přesah mezi komponentami.
Moduly	Jsou samostatnými celky řešení poskytující konkrétní funkcionality a jsou samostatně licencovány v rámci licence platformy ELDAx. Základním modulem je ELDAx/BASE obsažen v každé konfiguraci licence produktu ELDAx bez ohledu na pořízenou komponentu.
Konfigurátor	Konfigurátor licence slouží ke konfiguraci licence produktu ELDAx, vč. nacenění. Konfigurátor je dostupný pro partnery ELDAx v rámci licenčního programu EPP
EPP	ELDAx Partner Program je programem určeným pro kooperaci s partnery, kteří mohou platformu ELDAx dodávat, implementovat případně servisovat.
Nadstavba	Nadstavbou se rozumí produkt, který je integrovaný pomocí rozhraní ELDAx/SInRO na řešení ELDAx. Jedná se například o spisovou službu nebo další systémy využívající platformu ELDAx
ELDAx/SInRO	Standardní integrační rozhraní platformy ELDAx. Slouží pro komunikaci externích systémů s platformou a zároveň je možné přes něho platformu kompletně ovládat.
Agenda	Agenda je vytvořený soubor funkcionalit pokrývající konkrétní proces.

IDENTIFIKACE DOKUMENTU, ŘÍZENÍ ZMĚN

Verze	Popis změn	Datum	Zaznamenal
1.0	Iniciační dokument	19/05/2022	OH
1.0	Revidováno	13/01/2023	OH
1.1	Revidováno	30/06/2024	OH
1.1.1	Revidováno	13/12/2024	LV
1.2	Revidováno z důvodu výstupních formátů	01/06/2026	OH

OBSAH

1 UPOZORNĚNÍ A AUTORSKÁ PRÁVA

Tento dokument obsahující politiku provozu kvalifikované služby ELDAx Q-validation pro ověřování platnosti elektronických podpisů a pečetí je veřejně dostupným dokumentem ve vlastnictví společnosti Seyfor, a.s.

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 Seyfor, a.s. jako poskytovatele služby.

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.

2 ÚVOD

Tento dokument, Politika ELDAx Q-validation kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí (dále též „Politika“), představuje pravidla a postupy, které společnost Seyfor, a.s. uplatňuje v souladu s platnými právními předpisy a technickými normami pro zajištění provozu kvalifikované služby ELDAx Q-validation (dále jen ELDAx Q-validation, Q-validation nebo „kvalifikovaná služba“) pro ověřování kvalifikovaných elektronických podpisů a pečetí.

Zákonné požadavky kladené na službu ELDAx Q-validation jsou definovány:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- Zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- Zákonem č. 110/2019 Sb., o ochraně osobních údajů, v platném znění.

Kvalifikovaná služba ELDAx Q-validation, provozovaná společností Seyfor, a.s. coby kvalifikovaným poskytovatelem služeb vytvářejících důvěru, zajišťující ověřování elektronických podpisů a pečetí koncovým uživatelům a spoléhajícím se stranám (dále jen „Klient“) je poskytována všem Klientům na základě uzavřeného smluvního vztahu.

2.1 Přehled

Předmětem tohoto dokumentu, vypracovaného společností Seyfor, a.s., je představit a popsat politiku k poskytování služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí. 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.

Dokument je rozdělen do devíti kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty, které participují na poskytování služby ELDAx Q-validation a definuje přípustné využití služby.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace ke službě ELDAx Q-validation.
- Kapitola 4 definuje procesy životního cyklu služby ELDAx Q-validation, technické parametry, až po ukončení poskytování služby.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost včetně počítačové a síťové ochrany.
- Kapitola 7 je zaměřena na problematiku hodnocení poskytované služby ELDAx Q-validation.
- Kapitola 8 zahrnuje problematiku obchodní a právní, včetně ochrany osobních údajů.
- Kapitola 9 obsahuje závěrečná ustanovení.

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 kvalifikovaných elektronických podpisů a pečetí.

Bližší podrobnosti o kvalifikované službě ověřování platnosti kvalifikovaných elektronických podpisů a pečetí podle této Politiky mohou být uvedeny v odpovídající Prováděcí směrnici služby ELDAx Q-validation (dále též „Směrnice“).

2.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu:	Politika ELDAx Q-validation kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí, verze 1.0 – PUBLIC
OID politiky:	- není přiděleno -
Datum vydání:	28. 04. 2022
Doba platnosti:	Do odvolání nebo do dne ukončení provozu služby

2.3 Participující subjekty

2.3.1 Poskytovatel služby

Kvalifikovaným poskytovatelem kvalifikované služby vytvářející důvěru ELDAx Q-validation je společnost Seyfor, a.s.

2.3.2 Spoléhající se strany

Spoléhající se stranou je jakýkoli subjekt (fyzická osoba, právnická osoba nebo organizační složka státu), který uzavřel s poskytovatelem služby, společností Seyfor, a.s., smluvní vztah na využívání služby ELDAx Q-validation dle této Politiky.

2.3.3 Jiné participující strany

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

2.4 Použití služby ELDAx Q-validation

2.4.1 Přípustné použití služby

Službu ELDAx Q-validation lze využívat pouze v souladu s touto Politikou, s platnou legislativou a v souladu s garantovaným použitím této služby, tedy s řádnými a legálními účely procesů ověřování platnosti elektronických podpisů a pečetí.

Službu lze čerpat pouze prostřednictvím definovaných rozhraní a aplikací, které jsou Klientovi zpřístupněny.

2.4.2 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.

2.4.3 Omezení použití služby

Služba ELDAx Q-validation provozovaná dle této Politiky nesmí být používána v rozporu s přípustným použitím popsaným v kapitole 2.4.1 a dále pro jakékoliv nelegální účely.

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.

2.5 Správa politiky

2.5.1 Organizace spravující politiku nebo prováděcí směrnici

Za správu této Politiky, resp. jí odpovídající Směrnici, je zodpovědná společnost Seyfor, a.s.

2.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

Kontaktní osobou společnosti Seyfor, a.s., v souvislosti s touto Politikou, resp. s jí odpovídající Směrnicí, je Manažer bezpečnosti služby.

2.5.3 Subjekt zodpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů služeb vytvářejících důvěru

Rozhodování o souladu postupů společnosti Seyfor, a.s. s postupy jiných poskytovatelů služeb vytvářejících důvěru je plně v kompetenci ředitele společnosti Seyfor, a.s.

2.5.4 Postupy pro schvalování Politiky

V případě, že je potřebné provést změny a aktualizace v této Politice s ohledem na soulad dle kapitoly 2.5.3, stanovuje ředitel společnosti Seyfor, a.s. veškeré postupy pro jejich schválení a pro přípravu nové verze, včetně osoby, která je oprávněna veškeré tyto změny provést.

Schválení aktualizací a nabytí platnosti nové verze Politiky předchází její schválení ředitelem společnosti Seyfor, a.s.

2.6 Přehled použitých zkratek a pojmů

Pojem nebo zkratka	Vysvětlení
AdES	Advanced Electronic Signature - zaručený elektronický podpis splňující požadavky článku 26 Nařízení (EU) č. 910/2014

ASiC	Associated Signature Containers - Kontejner s přidruženým podpisem
CAdES	CMS Advanced Electronic Signatures - formát, vycházející z technické specifikace ETSI TS 103 173, resp. ETSI EN 319 122, využívaný pro podepsání/pečetění obecných dokumentů a binárních dat, u kterých není možné použít vložený podpis (např. ZFO datové zprávy)
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
DR	Disaster Recovery je plán obnovy provozu IT systémů po rozsáhlém výpadku zkracující dobu zásahu a chybovost při výpadku
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
ELDAx Q-validation	Kvalifikovaná služba vytvářející důvěru pro ověřování platnosti kvalifikovaných elektronických podpisů a pečetí poskytovaná kvalifikovaným poskytovatelem služeb vytvářejících důvěru Seyfor, a.s.
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

GDPR	General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679)
Kvalifikovaná služba	Kvalifikovaná služba ověřování platnosti elektronických podpisů a pečetí je kvalifikovaná služba vytvářející důvěru vytvořená a provozovaná kvalifikovaným poskytovatelem vytvářejícím důvěru Seyfor, a.s. pro ověřování kvalifikovaných elektronických podpisů a pečetí dle specifikací ETSI
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.
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
PAdES	PDF Advanced Electronic Signatures - formát, vycházející z technické specifikace ETSI TS 103 172, resp. ETSI EN 319 142, využívaný pro podepsání/pečetění dokumentů PDF a PDF/A
PDCA	Plan-Do-Check-Act - Plánování-Zavedení-Kontrola-Využití (Demingův cyklus) je metoda neustálého zlepšování či zdokonalování týkajícího se například procesů, kvality výrobků, služeb, aplikací atp.
PDF	Portable Document Format - přenosný formát dokumentů, je souborový formát vyvinutý firmou Adobe pro ukládání dokumentů nezávisle na softwaru i hardwaru, na kterém byly pořízeny
QTSP	Qualified Trust Service Provider - kvalifikovaný poskytovatel

	služeb vytvářejících důvěru
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
XAdES	XML Advanced Electronic Signatures - formát, vycházející z technické specifikace ETSI TS 103 171, resp. ETSI EN 319 132, využívaný pro podepsání/pečetění strukturovaných dokumentů s XML datovou strukturou
XML	eXtensible Markup Language - rozšiřitelný (obecný) značkovací jazyk, je formát dokumentů, který umožňuje přijímání a odesílání dat mezi různými programy či systémy, včetně externích softwarových modulů pro zpracování dat

3 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

3.1 Úložiště informací a dokumentace

Společnost Seyfor, a.s. zřizuje a provozuje interní úložiště informací a dokumentace.

3.2 Zveřejňování informací a dokumentace

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

- Adresa sídla společnosti:

  Seyfor, a.s.

  Traťová 574/1

  619 00 Brno - Horní Heršpice

  Česká republika

Společnost Seyfor, a.s. může bez udání důvodu zrušit nebo pozastavit přístup k některým zveřejněným informacím.

3.3 Periodicita zveřejňování informací

Společnost Seyfor, a.s. zveřejňuje informace s následující periodicitou:

- Politika služby ELDAx Q-validation - po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu a zahájením provozu služby dle nové Politiky
- Prováděcí směrnice služby ELDAx Q-validation - neprodleně
- Ostatní veřejné informace - není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytované služby vytvářející důvěru

Jakékoliv změny v používání služby jsou oznámeny Klientům prostřednictvím kontaktních údajů, které byly Klienty oznámeny a uvedeny společnosti Seyfor, a.s.

Jakékoliv změny v poskytování služby, včetně záměru o ukončení činnosti, oznámí společnost Seyfor, a.s. orgánu dohledu (Digitální a informační agentura) v souladu s eIDAS, článkem 24, odstavec 2, paragraf a).

3.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje společnost Seyfor, a.s. bezplatně bez omezení.

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

4 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ ELDAX Q-VALIDATION

4.1 Počáteční ověření identity

Služba ELDAx Q-validation je dostupná pouze pro subjekty, které mají se společností Seyfor, a.s. uzavřenou platnou Smlouvu o využívání této služby (dále též „Smlouva“).

4.1.1 Registrace uživatele služby

Pověřené osoby subjektu oprávněné pro získání přístupu ke službě ELDAx Q-validation jsou uvedeny ve Smlouvě. Tyto oprávněné osoby mohou požádat o přidělení osobních autentizačních údajů pro přístup ke službě ELDAx Q-validation.

4.1.2 Registrace IS jako Klienta služby

Pověřené osoby subjektu oprávněné pro získání přístupu ke službě ELDAx Q-validation jsou uvedeny ve Smlouvě. Tyto oprávněné osoby mohou požádat o přidělení autentizačních údajů pro automatizovaný přístup ke službě ELDAx Q-validation prostřednictvím webových služeb.

4.2 Autentizace ke službě

Autentizace přístupu uživatele nebo IS ke službě ELDAx Q-validation je možná pouze prostřednictvím Rozhraní pomocí přidělených autentizačních údajů. Autentizačními údaji pro službu ELDAx Q-validation je kombinace uživatelského jména a hesla.

4.3 Pozastavení či ukončení čerpání služby

V případě nedodržování podmínek pro využívání služby ELDAx Q-validation definovaných v této Politice je Poskytovatel oprávněn pozastavit přístup uživatele k této službě. V případě závažných pochybení je Poskytovatel oprávněn uživateli přístup ke službě ELDAx Q-validation ukončit.

Pozastavení, případně ukončení přístupu uživatele ke službě ELDAx Q-validation je uživateli oznámeno způsobem uvedeným ve Smlouvě.

4.4 Rušení uživatelských účtů

Rušení uživatelských účtů ke službě ELDAx Q-validation se provádí:

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

5 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY ELDAX Q-VALIDATION

Služba ELDAx Q-validation 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 (eIDAS) 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.

5.1 Uzavření Smlouvy

5.1.1 Subjekty oprávněné uzavřít Smlouvu

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

5.1.2 Proces uzavření Smlouvy a odpovědnosti

Klient hodlající využívat službu ELDAx Q-validation je povinen zejména:

- seznámit se s touto Politikou a smluvně se zavázat jednat podle ní,
- poskytovat pravdivé a úplné informace pro uzavření Smlouvy,
- překontrolovat, zda údaje uvedené ve Smlouvě jsou správné a odpovídají požadovaným údajům.

Poskytovatel služby, společnost Seyfor, a.s., je povinen zejména:

- před uzavřením Smlouvy informovat pověřené osoby druhé smluvní strany o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované platnou legislativou a technickými standardy,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.3,
- činnosti spojené se službou ELDAx Q-validation poskytovat v souladu s platnou legislativou, touto Politikou, příslušnou Směrnicí a provozní dokumentací.

5.2 Definice technických parametrů služby ELDAx Q-validation

5.2.1 Ověřované certifikáty

Služba ELDAx Q-validation provádí ověřování elektronických podpisů a elektronických pečetí založených na kvalifikovaných certifikátech dle nařízení eIDAS. Jedná se tedy o ověřování kvalifikovaných podpisů a pečetí (vytvořených prostřednictvím QSCD zařízení), případně zaručených podpisů a pečetí založených na kvalifikovaném certifikátu.

Kvalifikovanost jednotlivých kvalifikovaných certifikátů, resp. kvalifikovaných poskytovatelů služeb vytvářejících důvěru, kteří tyto kvalifikované certifikáty vydaly, je ověřována vůči důvěryhodným seznamům (TL, Trusted Lists). Seznam adres všech 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/tools/lotl/eu-lotl.xml

5.2.2 Ověřované formáty elektronických podpisů a pečetí

Služba ELDAx Q-validation 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 (případně PKCS#7)
  - Formát využívaný pro podepsání/pečetění dokumentů PDF a PDF/A
  - Technické specifikace: ETSI TS 103 172, resp. ETSI EN 319 142
- XAdES
  - Formát využívaný pro podepsání/pečetění strukturovaných dokumentů s XML datovou strukturou
  - Technické specifikace: ETSI TS 103 171, resp. ETSI EN 319 132
- CAdES
  - Formát využívaný pro podepsání/pečetění obecných dokumentů a binárních dat u kterých není možné použít vložený podpis
  - Technické specifikace: ETSI TS 103 173, resp. ETSI EN 319 122

Služba ELDAx Q-validation poskytuje podporu BASELINE úrovní jednotlivých ověřovaných elektronických podpisů a pečetí:

- BASELINE-B (Basic)
- BASELINE-T (Time)
- BASELINE-LT (Long Term)
- BASELINE-LTA (Long Term Archiving)

5.3 Validační proces

Jednotlivé typy elektronických podpisů a elektronických pečetí v podporovaných formátech uvedených v kapitole 4.2.2 umožňují různou úroveň ověřování platnosti elektronického certifikátu, na kterém je daný podpis/pečeť založena.

Z tohoto důvodu kvalifikovaná služba ELDAx Q-validation obsahuje několik úrovní validace pro různé typy podpisů/pečetí a informací v nich obsažených.

Dostupné 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.

Jednotlivé dostupné úrovně validace jsou následující:

- Proces ověření základních elektronických podpisů (Basic Signature)
- Proces ověření elektronických podpisů s časovým razítkem (Signature with Timestamp)
- Proces ověření elektronických podpisů s daty pro dlouhodobé ověření (Signature with Long-Term Validation Material)
- Proces ověření archivních formátů elektronických podpisů (Signature providing Long Term Availability and Integrity of Validation Material)

5.3.1 Výsledek validačního procesu

Pokud jsou ověřovaný elektronický podpis nebo elektronická 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.

Konkrétní výstup validačního procesu může nabývat hodnot:

- Platný (TOTAL-PASSED)
- Neplatný (TOTAL-FAILED)
- Nelze určit (INDETERMINATE)

Vyhodnocení procesu ověření platnosti elektronického podpisu či elektronické pečeti je přímo závislé na zvolené úrovni validace či 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. Pro vyhodnocení ověření je 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.

5.3.2 Výstup validačního procesu

Kvalifikovaná služba ELDAx Q-validation poskytuje výstup validačního procesu formou strukturovaných XML dat vhodných pro integraci do aplikací třetích stran a současně také umožňuje získat výsledek validačního procesu jako PDF dokument s lidsky čitelným výstupem. Uživatel služby ELDAx Q-validation si prostřednictvím jejího rozhraní může zvolit, jaký formát výsledku validace požaduje.

Vlastní odpověď rozhraní služby ELDAx Q-validation je z důvodů autenticity a ověřitelnosti odpovědi služby zabezpečena zaručenou elektronickou pečetí Poskytovatele.

5.3.2.1 Strukturovaná XML data

Pro integraci do navazujících informačních systémů nabízí služba ELDAx Q-validation výstup ve třech typech výstupních XML dokumentů, které si může uživatel při volání služby zvolit.

- Základní report (Simple Report)

- Obsahuje pouze základní zjednodušené informace o provedeném procesu ověření platnosti elektronických podpisů a pečetí pro všechny podpisy, pečeti a časová razítka v rámci dokumentu. Tato strukturovaná XML data jsou vždy opatřena zaručenou elektronickou pečetí Poskytovatele.

- Detailní report (Detailed Report)
  - Obsahuje podrobné informace o provedení a vyhodnocení všech kroků provedených v rámci validačního procesu pro všechny podpisy, pečeti a časová razítka v rámci dokumentu. Tato strukturovaná XML data jsou vždy opatřena zaručenou elektronickou pečetí Poskytovatele.
- Etsi report (Etsi Report)
  - Představuje validační report ve výstupním formátu a struktuře stanovené a definované normou ETSI TS 119 102-2. Tento report je dostupný pouze v datovém formátu XML.

5.3.2.2 PDF dokument

Pro snazší prezentaci výsledků validačního procesu koncovým uživatelům nabízí služba ELDAx Q-validation výstup ve formátu PDF. Služba nabízí dva typy výstupních PDF reportů, které svým obsahem odpovídají základním strukturovaným XML datům dle kapitoly 5.3.2.1.

- Základní report (Simple Report)
  - Obsahuje v grafické podobě interpretované informace v rozsahu dat odpovídajících strukturovanému výstupu XML Simple Report. Tento výstupní dokument je vždy opatřen zaručenou elektronickou pečetí Poskytovatele.
- Detailní report (Detailed Report)
  - Obsahuje v grafické podobě interpretované podrobné informace v rozsahu dat odpovídajících strukturovaného výstupu XML Detailed Report. Tento výstupní dokument je vždy opatřen zaručenou elektronickou pečetí Poskytovatele.

5.4 Interpretace výstupu validačního procesu

V rámci intepretace generovaných výstupů validační služby, které na základě zaslaného požadavku obdrží Klient služby ve formě validačních reportů, je nutné zmínit některá specifika, která je třeba brát v potaz v rámci návazných rozhodnutí jak s danými výstupy naložit.

5.4.1 Integrita dokumentu

V případě PDF dokumentu je integrita daného dokumentu chráněna posledním přidaným bezpečnostním prvkem (el. podpisem/pečetí), který pokrývá celkový dokument a tím jednoznačně zajišťuje jeho neměnnost. Pokud dokument obsahuje více než jeden bezpečnostní prvek, není z výstupu validačního procesu jednoznačně patrné, zda nedošlo k případným změnám na dokumentu mezi aplikací jednotlivých bezpečnostních prvků (inkrementální přidání obsahu do PDF dokumentu - změny typu poznámek, anotací, apod.), které nejsou součástí samotné podepsané části dokumentu – definované umístěním a délkou offsetu (ByteRange) jednotlivých bezpečnostních prvků. V tomto

případě mohou být předchozí bezpečnostní prvky validovány jako platné a neporušené, jelikož nebyla narušena jejich technická platnost (podpisová část se nezměnila), i když mohlo dojít ke změně vizuální podoby dokumentu po jejich aplikaci na dokument

Je doporučeno dokument validovat vždy po aplikaci každého jednotlivého bezpečnostního prvku, aby bylo zajištěno, že před dalším podpisem/pečetí nedošlo k jakýmkoliv úpravám daného dokumentu.

5.4.2 CRL seznamy

Kvalifikovaná služba ELDAx Q-validation si interně neukládá seznamy zneplatněných certifikátů, neboli CRL seznamy, jednotlivých certifikačních autorit a tudíž nedrží informaci o revokovaných certifikátech v případě, že dané CRL seznamy již nejsou dostupné přímo u dané certifikační autority. V tomto případě, kdy již dané seznamy nejsou volně k dispozici u příslušné certifikační autority, může dojít k interpretaci bezpečnostního prvku, který je založen na certifikátu od této certifikační autority, jako že již není jednoznačně platný.

5.5 Dostupnost služby

Dostupnost služby ELDAx Q-validation 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 poskytuje garantovanou minimální dostupnost ukotvenou ve Smlouvě o poskytování služby s koncovým Klientem.

5.6 Úschova dat o ověřování platnosti elektronických podpisů a pečetí

Doba, po kterou jsou uchovávány záznamy o provedeném ověření platnosti elektronických podpisů a pečetí, činí minimálně 10 let.

6 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Management bezpečnosti je zaměřen především na:

- systém poskytované služby ELDAx Q-validation,
- veškeré procesy podporující poskytování služby ELDAx Q-validation.

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech TOP 35, zahrnujícího oblasti celkové bezpečnostní politiky, plánu pro zvládání krizových situací a plánu obnovy, Prováděcí směrnice služby ELDAx Q-validation, tak v upřesňujících interních dokumentech.

6.1 Fyzická bezpečnost

6.1.1 Umístění a konstrukce

Kvalifikovaná služba ELDAx Q-validation je provozována v cloudovém prostředí společnosti Seyfor, a.s., které splňuje vysoké standardy na bezpečnost dle normy ISO 27001 a vysokou dostupnost dle mezinárodních standardů. Tato služba je oddělena ve své bezpečnostní zóně a není ovlivněna jiným zákazníkem v prostředí CLOUD.

Zařízení, na kterém je služba provozována, je spravováno certifikovanými zaměstnanci, kteří splňují certifikace a školení od společností Microsoft a VMware, Inc.

6.1.2 Fyzický přístup

Fyzický přístup do bezpečnostní zóny cloudového prostředí společnosti Seyfor, a.s. je řízen vnitřními směrnicemi zajišťujícími bezpečnost. Objekt společnosti je chráněn bezpečnostními poplachovými prvky a dále je kontrolován fyzickou bezpečností agenturou.

6.1.3 Elektřina a klimatizace

Datové centrum pro cloudové prostředí společnosti Seyfor, a.s., ve kterém je provozována kvalifikovaná služba ELDAx Q-validation, splňuje všechny požadavky výrobců hardwaru na systémy chlazení a napájení. Housing centrum je plně klimatizováno se stálou teplotou 20°C ± 5°C. Teplota v místnosti je snímána aktivními čidly, které jsou napojeny na monitorovací systém s poplachovým zařízením. Přívod elektřiny je vždy řešen pomocí dvou nezávislých zdrojů elektrické energie a jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

6.1.4 Vlivy vody

Architektura datového centra, ve kterém je provozována kvalifikovaná služba ELDAx Q-validation, splňuje veškerá opatření proti povětrnostním podmínkám, které by způsobily poškození hardware a tím narušily poskytování služby. V místnostech jsou umístěna čidla kontrolující vlhkost a výskyt vody, která jsou napojena na monitorovací systém s poplachovým zařízením.

6.1.5 Protipožární opatření a ochrana

Celý objekt, ve kterém se nachází datové centrum pro poskytování služby kvalifikované ELDAx Q-validation, je opatřen protipožárním zařízením napojeným na monitorovací systém vyhlašující

poplach Záchrannému hasičskému sboru. Místnost je vybavena hasičskými přístroji pro hašení elektroniky.

6.1.6 Ukládání médií

Všechna paměťová zařízení a papírová dokumentace obsahující data jsou uložena na bezpečném místě v sídle společnosti Seyfor, a.s. Do těchto prostor mají přístup pouze povolené osoby a to dle interních směrnic společnosti. Kopie všech dokumentů a médií, pokud je požadováno, jsou ukládány v geograficky oddělené lokalitě, ke které má přístup pouze oprávněný pracovník společnosti.

6.1.7 Nakládání s odpady

Veškerý odpad vznikající v rámci poskytování kvalifikované služby ELDAx Q-validation je na pracovištích společnosti Seyfor, a.s. skartován a následně likvidován odbornou společností.

6.1.8 Zálohy mimo budovu

Zálohy provozních a pracovních kopií jsou uloženy na místě určeném interní směrnicí společnosti Seyfor, a.s. a mohou k nim přistupovat pouze oprávnění pracovníci.

6.2 Procesní bezpečnost

6.2.1 Důvěryhodné role

Důvěryhodné role vyplývají z pracovních činností na základě interní směrnice společnosti Seyfor, a.s. a jsou v souladu s bezpečnostními pravidly.

6.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Počet osob požadovaných na zajištění jednotlivých činností je vždy minimálně 2 na jednu činnost a to vždy tak, aby se osoby byly schopny zastupovat v rámci všech přiřazených povinností. Tímto je pro poskytovanou službu vždy zaručena dostupnost lidských zdrojů k zajištění podpory provozu.

6.2.3 Identifikace a autentizace pro každou roli

Každá osoba s přidělenou rolí je opatřena autentifikačním certifikátem a heslem pro VPN připojení do cloudového prostředí, ve kterém je poskytována kvalifikovaná služba ELDAx Q-validation. Autorita pro vydávání certifikátů je ve výhradní kontrole společnosti Seyfor, a.s.

6.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interní směrnici společnosti Seyfor, a.s.

6.3 Personální bezpečnost

6.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Požadavky na kvalifikaci zaměstnanců pro práci s kvalifikovanou službou ELDAx Q-validation vychází z pracovních pozic popsaných v interní směrnici společnosti Seyfor, a.s.

6.3.2 Posouzení spolehlivosti osob

Před obsazením pracovníků do rolí v rámci kvalifikované služby ELDAx Q-validation je nezbytné posoudit jejich způsobilost. Zdrojem informací o zaměstnancích, nutných pro tato posouzení, jsou:

- Samotný pracovník
- Osoby, které pracovníka znají, se kterými pracoval a jeho nadřízení
- Veřejně přístupné informační zdroje

Prvotní informace jsou poskytnuty samotnými pracovníky při osobním pohovoru v rámci přijímání do pracovního poměru ve společnosti. Tyto informace jsou aktualizovány při pravidelných pohovorech s nadřízenými pracovníky v průběhu celého pracovního poměru.

V rámci posuzování vhodnosti a spolehlivosti pracovníka pro konkrétní roli může být vznesen i požadavek na prokázání bezúhonnosti. Ta je posuzována podle výpisu z rejstříku trestů. V souladu se zavedenými postupy pro nábor zaměstnanců do společnosti poskytuje každý pracovník tyto informace v průběhu vstupního osobního pohovoru.

6.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci společnosti Seyfor, a.s., kteří se podílejí na provozu, správě a rozvoji kvalifikované služby ELDAx Q-validation, jsou odborně zaškoleni. Toto zaškolení se provádí kombinací samostudia a metodického vedení již zaškoleným pracovníkem.

U určených rolí může být školení nahrazeno prokazatelným seznámením pracovníka s dokumenty upravujícími provoz kvalifikované služby se vztahem k dané příslušné roli. Požadavky a specifikace těchto rolí jsou uvedeny v interních směrnicích.

Školení zahrnuje nejen oblasti informační bezpečnosti systému, ochrany osobních údajů a dalších relevantních témat, ale také chování a postupy v případě havarijních situací.

O provedení školení musí být proveden písemný zápis.

6.3.4 Požadavky a periodicita školení

Pracovníci, kteří se podílejí na provozu, správě a rozvoji kvalifikované služby ELDAx Q-validation, musí projít dodatečným školením, kdykoliv jsou v rámci provozu kvalifikované služby implementovány nové vlastnosti a funkcionality.

Pracovníci jsou dále povinni v rámci přidělené role udržovat a zvyšovat svoji kvalifikaci, k čemuž jsou jim poskytovány aktuální informace o vývoji v předmětné oblasti, pokud jsou k dispozici.

Pravidelná školení pracovníků probíhají minimálně jednou za 12 měsíců.

6.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti a pro případ krizových situací jsou zaměstnanci podporováni k získávání znalostí potřebných pro výkon různých důvěryhodných rolí v rámci společnosti, nicméně výměny osob mezi jednotlivými rolemi nejsou prováděny.

6.3.6 Postihy za neoprávněné činnosti zaměstnanců

Při jakékoliv neautorizované činnosti či operaci, které jsou provedeny pracovníky v rolích správy a jsou považovány za hrubé porušení pracovní kázně a bezpečnostní incident, je s daným zaměstnancem postupováno odpovídajícím způsobem dle interních dokumentů společnosti.

6.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Společnost Seyfor, a.s. může nebo musí některé své činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami s danými dotčenými subjekty. Jedná se např. o zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory, apod.

Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými politikami, relevantními částmi interní dokumentace společnosti Seyfor, a.s., které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončen smluvní vztah a spolupráce.

6.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci společnosti Seyfor, a.s. mají k dispozici, kromě této Politiky a Směrnice kvalifikované služby ELDAx Q-validation a bezpečnostní a provozní dokumentace, i veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti v rámci přidělených rolí.

6.4 Auditní záznamy (logy)

6.4.1 Typy zaznamenávaných událostí

Systém kvalifikované služby ELDAx Q-validation zaznamenává informace o všech provedených operacích, včetně operací provedených správci systému, spolu s údaji o jeho stavu a provozu. Zaznamenávány jsou 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 integritu těchto 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.

6.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a zpracovávány v intervalech daných a definovaných v rámci interní dokumentace, nebo okamžitě v případě podezření či následně po bezpečnostním incidentu. Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem.

6.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu nejméně deseti let, nestanoví-li jiná relevantní legislativní norma či předpis jinak.

eIDAS SMART TRUST eLECTRONIC PLATFORM

6.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy způsobem zajišťujícím ochranu proti krádeži, modifikaci a zničení (ať již úmyslným nebo neúmyslným).

Auditní záznamy jsou vytvářeny a uchovávány v elektronické podobě a o jejich ochranu se stará aplikace ELDAx. Tato aplikace je certifikována pro ukládání citlivých údajů a s aplikovaným řízeným přístupem odpovědných fyzických osob tvoří bezpečnostní prvek pro ochranu auditních záznamů.

6.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy v elektronické podobě jsou zálohovány standardním způsobem, obdobně jako zálohovaní ostatních elektronických informací. Zálohování auditních záznamů v papírové formě není prováděno.

6.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Shromažďování auditních systémů v rámci systému kvalifikované služby probíhá interně dle interních pravidel společnosti.

6.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt, který způsobil zápis události do auditního záznamu, není o dané události informován.

6.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je v rámci společnosti Seyfor, a.s. prováděno v pravidelných periodických intervalech coby součást analýzy rizik. Veškerá závažná porušení bezpečnosti jsou neprodleně eskalována odpovědné osobě, případně organizační složce.

6.5 Uchovávání informací a dokumentace

Procesy a mechanismy uchovávání informací a dokumentace jsou prováděny dle interních předpisů, které upravují tuto předmětnou oblast.

6.5.1 Typy informací a dokumentace, které se uchovávají

V rámci provozu kvalifikované služby ELDAx Q-validation uchovává společnost Seyfor, a.s. níže uvedené informace určené pro účely auditu:

- Data výsledků provedených validací kvalifikovaných elektronických podpisů a pečetí
- Transakční záznamy o provedených operacích
- Související smluvní dokumentace pro přístup ke službě
- Aplikační programové vybavení, provozní a bezpečnostní dokumentace

Dokumenty poskytnuté službě ELDAx Q-validation k provedení ověření platnosti elektronických podpisů a pečetí nejsou uchovávány.

6.5.2 Doba uchování uchovávaných informací a dokumentace

Informace a dokumentace vztahující se k poskytované kvalifikované službě ELDAx Q-validation jsou uchovávány minimálně po dobu deseti let.

eIDAS SMART TRUST eLECTRONIC PLATFORM

6.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Data a dokumenty v archivu jsou chráněny způsobem odpovídajícím jejich bezpečnostní citlivosti a významu, konkrétně dle národního standardu o archivnictví.

6.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací postupy pro uchovávání informací a dokumentace jsou upraveny interní dokumentací společnosti Seyfor, a.s.

6.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že jsou v rámci kvalifikované služby ELDAx Q-validation využívána elektronická časová razítka, jedná se o kvalifikovaná elektronická časová razítka vydaná zvoleným kvalifikovaným poskytovatelem služeb vytvářejících důvěru (QTSP).

6.5.6 Postupy pro získání a ověření uchovávaných informací a dokumentace

Přístup k uchovávaným informacím a dokumentům, které jsou umístěny v lokalitách k tomu určených, mají pouze:

- Pracovníci společnosti Seyfor, a.s., pokud je to v rámci jejich role vyžadováno
- Oprávněné kontrolní subjekty (členové nezávislého auditního týmu), orgány činné v trestním řízení a soudy, pokud je to právními normami vyžadováno

O každém takto povoleném přístupu je pořizován písemný záznam.

6.6 Obnova po havárii nebo kompromitaci

6.6.1 Postup v případě incidentu a kompromitace

V případě výskytu bezpečnostního incidentu, či havárie, postupuje společnost Seyfor, a.s. v souladu s postupy uvedenými v interním dokumentu DR (Disaster Recovery) plánu, případně v dalších relevantních dokumentech.

V případě, že dojde k bezpečnostnímu incidentu, který bude mít přímý dopad na funkčnost nebo důvěryhodnost samotné služby, je společnost Seyfor, a.s. povinna zveřejnit informace o bezpečnostním incidentu na internetové adrese podle kapitoly 3.2, kontaktovat a informovat o bezpečnostním incidentu všechny případné dotčené Klienty a dále eskalovat daný incident a reportovat jej certifikační autoritě a to nejpozději do 24 hodin od daného incidentu. V případě závažného incidentu, kdy služba nebude nadále v souladu s Nařízením eIDAS na který je certifikována, bude incident reportován i orgánu dohledu.

6.6.2 Poškození výpočetních prostředků, software nebo dat

Postupy jsou uvedeny v interním dokumentu DR (Disaster Recovery) plánu, případně v dalších relevantních dokumentech.

6.6.2.1 Schopnost obnovit činnost po havárii

Postupy jsou uvedeny v interním dokumentu DR (Disaster Recovery) plánu, případně v dalších

relevantních dokumentech.

6.7 Ukončení činnosti poskytovatele služeb

Pro ukončování činnosti kvalifikovaného poskytovatele služby vytvářející důvěru (QTSP) platí následující pravidla:

- ukončení činnosti kvalifikovaného poskytovatele služby vytvářející důvěru bude písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu na využívání kvalifikované služby ELDAx Q-validation a to nejpozději s 3 měsíčním předstihem,
- ukončení činnosti poskytovatele služby vytvářející důvěru bude zveřejněno na internetové adrese podle kapitoly 3.2,
- 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. Tento připravený plán je součástí přílohy č. 13 interního dokumentu TOP 34.

Osobou zodpovědnou za aktivaci plánu je ředitel společnosti Seyfor, a.s.

Realizaci jednotlivých kroků zajišťuje Garant (vlastník) kvalifikované služby, který nese zodpovědnost za jejich uskutečnění dle schváleného plánu.

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

- informace o odnětí statutu bude písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu na využívání kvalifikované služby ELDAx Q-validation,
- informace o odnětí statutu bude zveřejněna v souladu s kapitolou 3.2,
- o dalším postupu rozhodne ředitel společnosti Seyfor, a.s. na základě rozhodnutí orgánu dohledu.

V případě bankrotu je pokračováno v souladu s příslušnou legislativou.

7 TECHNICKÁ BEZPEČNOST

V této následující kapitole jsou definovány konkrétní bezpečnostní požadavky na jednotlivé oblasti pro zajištění kvality poskytované kvalifikované služby ELDAx Q-validation dle této Politiky.

7.1 Počítačová bezpečnost

7.1.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň pro zajištění bezpečnosti použitých systémů a komponent pro kvalifikovanou službu ELDAx Q-validation je definována platnou legislativou, respektive v ní odkazovaných technických standardech nebo normách.

7.1.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti kvalifikované služby ELDAx Q-validation 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

7.2 Bezpečnost životního cyklu

7.2.1 Řízení vývoje systému služby ELDAx Q-validation

Při vývoji systému kvalifikované služby ELDAx Q-validation je postupováno v souladu s best practice postupy pro vývoj software a dále v souladu s interní dokumentací.

7.2.2 Kontrola řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými periodickými audity jednou za rok a kontrolami bezpečnostní shody externí auditní společností.

7.2.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je ve společnosti Seyfor, a.s. 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.

7.3 Síťová bezpečnost

Kvalifikovaná služba ELDAx Q-validation je poskytována koncovým uživatelům pomocí internetu a pro zajištění bezpečné komunikace se požívá protokol HTTPS. Pro zajištění ochrany proti útoku cizím softwarem je použit firewall, který je schopen definovat povolené adresy uživatelů.

7.4 Ochrana proti padělání a odcizení dat

Systém pro zajištění ochrany dat proti jejich padělání a odcizení je navržen přímo v rámci kvalifikované služby ELDAx Q-validation, která využívá autentifikaci povolených uživatelů. Ve spojení s pravidelným auditem logů tvoří systém ochranu proti padělání a odcizení dat.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení podle Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 (eIDAS), včetně okolností pro provádění hodnocení, je striktně dána požadavky tohoto nařízení. Na základě těchto požadavků jsou další pravidelné audity akreditovaným posuzovatelem shody prováděny vždy v intervalu nepřekračujícím dva roky (24 měsíců).

V případě jakékoliv změny v softwarovém či hardwarovém vybavení, na kterém je kvalifikovaná služba ELDAx Q-validation poskytována, musí být zkoumán dopad těchto změn na kvalitu a bezpečnost služby.

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.

8.2 Identita a kvalifikace hodnotitele

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

8.3 Vztah hodnotitele a hodnoceného subjektu

Pravidelná kontrola provozu je prováděna vlastními interními pracovníky společnosti Seyfor, a.s., a vždy platí, že daný interní hodnotitel není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz kvalifikované služby ELDAx Q-validation.

V případě externího hodnotitele platí, že se jedná o subjekt, který není se společností Seyfor, a.s. majetkově ani organizačně svázán.

8.4 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.

8.5 Postup v případě zjištění nedostatků

V případě zjištění nedostatků v rámci prováděných hodnocení je informován bezpečnostní manager, a tyto nedostatky jsou komunikovány v rámci auditní zprávy. Bezpečnostní manager je povinen zajistit odstranění takto nalezených nedostatků, kdy dle jejich charakteru jsou naplánovány a provedeny nezbytné činnosti pro jejich odstranění a to jak technického charakteru (implementace dalších opatření, konfigurační změny, apod.), případně je provedena aktualizace relevantní dokumentace.

Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat kvalifikovanou službu ELDAx Q-validation, přeruší společnost Seyfor, a.s. tuto službu do doby, než budou tyto nedostatky odstraněny.

eIDAS SMART TRUST eLECTRONIC PLATFORM

8.6 Sdělování výsledků hodnocení

Výsledek a skutečnosti zjištěné v rámci hodnocení získaného auditem jsou formou písemné auditní zprávy prezentovány vedení společnosti Seyfor, a.s., které přijme konkrétní opatření vyplývající z daného auditního zjištění. S výsledkem je dále seznámen také bezpečnostní manager společnosti.

Sdělování výsledků hodnocení podléhá požadavkům legislativy.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za využívání služby ELDAx Q-validation

Poplatky za využívání kvalifikované služby ELDAx Q-validation jsou součástí Smlouvy uzavřené mezi Klientem a Poskytovatelem služby - společností Seyfor, a.s.

9.2 Citlivost obchodních informací

9.2.1 Výčet citlivých informací

Za citlivé a důvěrné jsou považovány veškeré informace, které jsou svojí povahou neveřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 3.2, jedná se zejména o:

- veškeré informace týkající se procesu ověřování, uložené v rámci služby - včetně auditních záznamů,
- veškeré soukromé klíče, používané v rámci procesu poskytování služby ELDAx Q-validation,
- veškeré obchodní informace společnosti Seyfor, a.s.,
- veškeré interní informace a dokumentace,
- výsledky externích i interních auditů služby,
- veškeré osobní údaje.

Citlivé informace mohou být zveřejněny pouze v souladu s touto politikou nebo zákonnými normami České republiky a jsou chráněny technickými a administrativními prostředky. Jejich zveřejnění mimo povolenou mez je považováno za hrubé porušení této Politiky, případně dalších souvisejících předpisů.

9.2.2 Informace mimo rámec citlivých informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 3.2.

9.2.3 Odpovědnost za ochranu citlivých informací

Každý zaměstnanec společnosti Seyfor, a.s., který přijde do styku či jinak nakládá s citlivými a důvěrnými informacemi uvedenými v kapitole 8.2.1 je zodpovědný za jejich ochranu a nesmí je bez souhlasu vlastníka služby či vedení společnosti poskytovat třetí straně.

9.3 Ochrana osobních údajů

Společnost Seyfor, a.s. zajišťuje ochranu osobních údajů osob a dalších neveřejných informací, k nimž získá přístup při uzavření smluvního vztahu s Klientem či v rámci provozu kvalifikované služby ELDAx Q-validation, v souladu s požadavky vzešlých z příslušných zákonných norem.

Zásady ochrany osobních údajů jsou obsaženy v této Politice, a v příloze č. 10 interního dokumentu TOP 36, a vycházejí z obecně závazných právních předpisů České republiky, zejména Nařízení

eIDAS SMART TRUST eLECTRONIC PLATFORM

Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, zkráceně zvané GDPR, a zákona č. 110/2019 Sb., o zpracování osobních údajů.

Zaměstnanci společnosti, případně subjekty definované platnou legislativou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích, datech a bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systému poskytujícího kvalifikovanou službu ELDAx Q-validation, jsou chráněny autorskými právy společnosti Seyfor, a.s., a představují její významné know-how a práva duševního vlastnictví.

9.5 Zřeknutí se záruk

Společnost Seyfor, a.s. důsledně odmítá jakékoliv záruky za provoz kvalifikované služby ELDAx Q-validation a výstupy dané služby, pokud byla tato služba a/nebo její rozhraní použito v rozporu s podmínkami využívání kvalifikované služby ELDAx Q-validation nebo s touto Politikou.

9.6 Omezení odpovědnosti

Společnost Seyfor, a.s. neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti požadované touto Politikou, podle které byla kvalifikovaná služba ELDAx Q-validation poskytována. Dále neodpovídá za škody vzniklé v důsledku porušení závazků Seyfor, a.s. z důvodu vyšší moci.

9.7 Odpovědnost za škodu, náhrada škody

Pro poskytování kvalifikovaných služeb vytvářejících důvěru platí relevantní ustanovení platné legislativy a dále takové záruky, které mohly být sjednány smlouvou mezi společností Seyfor, a.s. a uživatelem kvalifikované služby ELDAx Q-validation. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v elektronické nebo listinné formě.

Společnost Seyfor, a.s. se zavazuje:

- že splní veškeré povinnosti definované jak platnou legislativou, tak příslušnými politikami,
- že poskytne výše uvedené záruky po celou dobu platnosti Smlouvy o poskytování kvalifikované služby ELDAx Q-validation,
- že další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud.

Společnost Seyfor, a.s. neodpovídá:

- za vady poskytnuté služby vzniklé z důvodu nesprávného nebo neoprávněného využívání služby poskytnuté v rámci plnění Smlouvy o poskytování kvalifikované služby ELDAx Q-validation 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.

Případnou reklamaci poskytované služby ELDAx Q-validation je možné podat následujícími způsoby:

- e-mailem na adresu reklamace@seyfor.cz,
- prostřednictvím datové schránky společnosti Seyfor, a.s.,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba, pověřená osoba ve Smlouvě, je povinna uvést:

- co nejvýstižnější popis závady,
- bližší popis reklamované služby
- požadovaný způsob vyřízení reklamace.

O reklamaci společnost Seyfor, a.s. rozhodne nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, prostřednictvím datové schránky, jedná-li se o orgán státní správy, nebo doporučenou poštovní zásilkou), pokud se strany nedohodnou jinak.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do jednoho měsíce ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

V případě poskytované kvalifikované služby, je důkazní břemeno na straně kvalifikovaného poskytovatele služeb vytvářejících důvěru (QTSP) a je jeho právem prokázat, že škoda nastala bez jeho úmyslu nebo nedbalosti.

Ke krytí případných škod má společnost Seyfor, a.s. sjednané pojištění odpovědnosti.

9.8 Doba platnosti, ukončení platnosti

9.8.1 Doba platnosti

Tento dokument Politiky nabývá platnosti datem vydání uvedeným v kapitole 1.2.

Dokument Politiky zůstává v platnosti minimálně po dobu poskytování kvalifikované služby ELDAx Q-validation, nebo do okamžiku jejího nahrazení novou verzí.

9.8.2 Ukončení platnosti

Jedinou osobou, která je oprávněná schvalovat ukončení platnosti této Politiky, stejně jako její veškeré aktualizace, je ředitel společnosti Seyfor, a.s.

9.9 Komunikace mezi zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může společnost Seyfor, a.s. využít všechny typy kontaktů jako jsou dodané e-mailové adresy, poštovní adresy, datové schránky, telefonní

čísla, osobní jednání atd.

Komunikovat se společností Seyfor, a.s. lze taktéž způsoby uvedenými v kapitole 3.2 této Politiky.

9.10 Změny Politiky

9.10.1 Postup při změnách

Společnost Seyfor, a.s. je oprávněna v budoucnu doplnit či aktualizovat tuto Politiku o nová ustanovení, jejichž potřeba bude teprve zjištěna. Případné změny či aktualizace nebudou mít retrospektivní platnost.

V případě jakýchkoliv změn v tomto dokumentu musí být vždy změněna jeho verze.

9.10.2 Postup při oznamování změn

Jakékoliv případné změny (návrh nového znění), vydání nové verze Politiky, budou neprodleně zveřejněny na informační adrese, určené k publikaci veřejných informací o společnosti, definované v kapitole 3.2 této Politiky.

9.10.3 Souhlas se změnami

Klient využívající kvalifikovanou službu ELDAx Q-validation, na základě platného smluvního vztahu, je povinen se se zveřejněnými změnami a návrhem nové verze Politiky seznámit a v případě souhlasu se zavázat jednat v souladu s těmito změnami.

Návrh nového znění příslušných podmínek je možné kdykoliv před datem jejich účinnosti písemně odmítnout. Pokud tak nebude ze strany Klienta učiněno, platí, že navrhované změny přijímá. Pokud navrhované změny písemně odmítne, má rovněž právo písemně vypovědět Smlouvu, na jejímž základě byla kvalifikovaná služba ELDAx Q-validation poskytnuta, a to bezúplatně a s okamžitou účinností.

9.11 Změny služby

V případě, že jsou navrženy a plánovány implementační či procesní změny v rámci kvalifikované služby ELDAx Q-validation, které budou mít přímý dopad na její certifikovanost - služba nebude nadále v souladu s požadavky Nařízení eIDAS na které je certifikována, je společnost Seyfor, a.s. povinna před implementací takovýchto změn informovat certifikační autoritu a dále orgán dohledu a uskutečnit recertifikaci služby zahrnující takto plánované změny.

9.12 Řešení sporů

Jakýkoliv spor, který nastane v souvislosti s kvalifikovanou službou ELDAx Q-validation, a pro který se nepodaří naleznout smírné řešení, bude předmětem soudního rozhodnutí.

V případě snahy o vyřešení sporu mimosoudní cestou je ze strany Klienta možné použít následující stupně odvolání pro podání návrhu řešení, a to buď v elektronické, nebo listinné formě:

- Odpovědný pracovník společnosti Seyfor, a.s.
- Ředitel společnosti Seyfor, a.s.

Řešení veškerých sporů právního charakteru bude podstoupeno soudnímu rozhodnutí. Soudní jednání se bude konat na území České republiky v českém jazyce.

9.13 Rozhodné právo

Rozhodným právem pro řešení sporů, spojených s obchodní činností společnosti Seyfor, a.s., je legislativa České republiky.

9.14 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.