

Kvalifikovaný poskytovatel služeb vytvářejících důvěru elidentity a.s.

ACAeID 10.4 Certifikační politika - TSA

Verze:	1.1
Odpovídá:	Milan Berka
Datum:	17. 10. 2017
Utajení:	Veřejný dokument



Copyright © 2017 eidentity a.s.

Žádná část tohoto dokumentu nesmí být kopírována žádným způsobem bez písemného souhlasu majitelů autorských práv.

Některé názvy produktů a společností citované v tomto díle mohou být ochranné známky příslušných vlastníků.

Schváleno:

Verze	Schválil	
1.1	Ladislav Šedivý	

Historie dokumentu:

Verze	Datum	Autor	Poznámka
1.0	14. 3. 2010	Jiří Hejl	Certifikační politika autority vydávající časová razítka
1.0	14. 3. 2017	Milan Berka	Úprava vzhledem ke změně zákona a Nařízení eIDAS
1.1	08. 08. 2017	Milan Berka	Zpracování připomínek auditu a dozorového orgánu
	17. 10. 2017	Michal Příhoda	Aktualizace v souvislosti s novými klíči a root certifikátem

OBSAH

1	Úvod	7
2	Seznam použitých pojmů a zkratk	8
2.1	Rejstřík zkratk	8
2.2	Rejstřík pojmů	8
3	Základní pojetí	10
3.1	Služby autority časových razítek (TSA)	10
3.2	Autorita časových razítek	10
3.3	Zákazníci a odběratelé služby časového razítka	11
3.4	Spoléhající se strany	11
4	Politika TSA	12
4.1	Základní popis	12
4.2	Identifikace	12
4.3	Určení politiky a její použitelnosti	13
4.4	Hodnocení shody a jiná hodnocení	13
4.4.1	Periodicita hodnocení	13
4.4.2	Identita a kvalita hodnotitele	13
4.4.3	Vztah hodnotitele k hodnocené entitě	13
4.4.4	Hodnocené oblasti	13
4.4.5	Postupy v případě zjištění nedostatku	13
4.4.6	Sdělování výsledků hodnocení	14
5	Závazky a odpovědnosti	15
5.1	Závazky TSA	15
5.1.1	Obecné závazky TSA	15
5.1.2	Závazky TSA ve vztahu k žadatelům o kvalifikované elektronické časové razítko a držitelům kvalifikovaných elektronických časových razítek	15
5.2	Závazky žadatelů o kvalifikované elektronické časové razítko a držitelů kvalifikovaného časového razítka	16
5.3	Závazky spoléhajících se stran	16
5.4	Odpovědnost	16
6	Požadavky na postupy a procesy TSA	18
6.1	Správa politiky	18
6.1.1	Organizace spravující politiku a prováděcí směrnici TSA	18
6.1.2	Kontaktní osoba spravující tento dokument	18
6.1.3	Postupy při schvalování tohoto dokumentu	18
6.2	Požadavky na životní cyklus párových dat TSA	19
6.2.1	Generování a instalace párových dat	19
6.2.1.1	Generování párových dat	19
6.2.1.2	Vlastnosti kryptografického modulu	19
6.2.1.3	Poskytování veřejných klíčů	19
6.2.1.4	Délky párových dat	19
6.2.2	Ochrana soukromého klíče TSA (dat pro vytváření elektronických značek)	19
6.2.2.1	Standardy a podmínky používání kryptografického modulu	19
6.2.2.2	Zálohování soukromých klíčů	19
6.2.2.3	Uchovávání soukromých klíčů	20
6.2.2.4	Transfer soukromých klíčů	20
6.2.2.5	Uložení soukromých klíčů v kryptografickém modulu	20
6.2.2.6	Aktivační data	20
6.2.2.7	Postup při aktivaci soukromých klíčů	20
6.2.2.8	Postup při deaktivaci soukromých klíčů	20
6.2.2.9	Postup při zničení soukromých klíčů	20

6.2.3	Distribuce veřejných klíčů	20
6.2.4	Žádost o certifikáty TSA.....	20
6.2.4.1	Profil certifikátu.....	21
6.2.5	Výměna párových dat	21
6.2.6	Ukončení životního cyklu párových dat	21
6.2.6.1	Zneplatnění a pozastavení platnosti certifikátu	22
6.2.7	Správa kryptografického modulu používaného při vytváření kvalifikovaných časových razítek	22
6.2.7.1	Hodnocení kryptografického modulu.....	22
6.3	Vydávání kvalifikovaných elektronických časových razítek	22
6.3.1	Uzavření smlouvy a registrační proces.....	22
6.3.2	Zpracování žádosti o kvalifikované elektronické časové razítko	22
6.3.2.1	Identifikace a autentizace.....	22
6.3.2.2	Přijetí nebo zamítnutí žádosti o kvalifikované elektronické časové razítko.....	23
6.3.2.3	Doba zpracování žádosti o kvalifikované elektronické časové razítko.....	23
6.3.3	Vydání kvalifikovaného časového razítka	23
6.3.3.1	Úkony TSA v průběhu vydávání kvalifikovaného časového razítka.....	23
6.3.3.2	Oznámení o vydání kvalifikovaného časového razítka žadateli o vydání kvalifikovaného časového razítka.....	23
6.3.3.3	Převzetí kvalifikovaného časového razítka	24
6.3.4	Ověření kvalifikovaného časového razítka	24
6.3.5	Platnost kvalifikovaného časového razítka	24
6.3.6	Struktura žádosti, odpovědi a kvalifikovaného časového razítka	25
6.3.6.1	Struktura žádosti o kvalifikované elektronické časové razítko	25
6.3.6.2	Struktura odpovědi na žádost o kvalifikované elektronické časové razítko	26
6.3.6.3	Struktura kvalifikovaného časového razítka	27
6.3.7	Synchronizace měřidla času s UTC.....	27
6.3.7.1	Synchronizace.....	27
6.3.7.2	Bezpečnost měřidla času	28
6.3.7.3	Detekce odchýlení měřidla času	28
6.3.7.4	Přestupná sekunda	28
6.4	Správa a provozní bezpečnost TSA.....	28
6.4.1	Řízení bezpečnosti	28
6.4.2	Hodnocení a řízení rizik	28
6.4.3	Personální bezpečnost	28
6.4.3.1	Důvěryhodné role	29
6.4.3.2	Role vyžadující rozdělení pravomocí	29
6.4.3.3	Požadavky na personál.....	29
6.4.3.4	Požadavky na nezávislé dodavatele	30
6.4.3.5	Dokumentace poskytovaná zaměstnancům	30
6.4.4	Fyzická bezpečnost a bezpečnost prostředí.....	30
6.4.4.1	Umístění a konstrukce	30
6.4.4.2	Fyzický přístup	30
6.4.4.3	Elektřina a klimatizace	30
6.4.4.4	Vliv vody	31
6.4.4.5	Protipožární opatření a ochrana.....	31
6.4.4.6	Ukládání médií	31
6.4.4.7	Nakládání s odpady.....	31
6.4.4.8	Zálohy mimo budovu provozního prostředí.....	31
6.4.5	Řízení provozu.....	31
6.4.5.1	Specifické technické požadavky na počítačovou bezpečnost	31

6.4.5.2	Hodnocení počítačové bezpečnosti	32
6.4.6	Řízení přístupu do systému	32

6.4.7	Vývoj a údržba důvěryhodných systémů	32
6.4.7.1	Řízení vývoje systému	32
6.4.7.2	Kontroly řízení bezpečnosti	32
6.4.8	Obnova po havárii nebo kompromitaci	33
6.4.8.1	Postup v případě havárie nebo kompromitace	33
6.4.8.2	Poškození výpočetních prostředků, software nebo dat	33
6.4.8.3	Postup při zjištění odchýlení měřidla času	33
6.4.8.4	Kompromitace soukromého klíče TSA	33
6.4.8.5	Kompromitace soukromého klíče nadřízené certifikační autority	34
6.4.8.6	Schopnost obnovit činnost po havárii	34
6.4.9	Ukončení činnosti TSA	34
6.4.10	Shoda s právními předpisy	34
6.4.11	Záznam informací o provozu TSA	34
6.4.11.1	Typy zaznamenávaných informací	34
6.4.11.2	Periodicita zpracování záznamů	35
6.4.11.3	Doba uchování auditních záznamů	35
6.4.11.4	Ochrana auditních záznamů	35
6.4.11.5	Postupy pro zálohování auditních záznamů	35
6.4.11.6	Systém shromažďování auditních záznamů (interní nebo externí)	35
6.4.11.7	Postup při oznamování události subjektu, který ji způsobil	35
6.4.11.8	Hodnocení zranitelnosti	35
6.4.12	Uchovávání informací a dokumentace	35
6.4.12.1	Typy informací a dokumentace, které se uchovávají	35
6.4.12.2	Doba uchování uchovávaných informací a dokumentace	36
6.4.12.3	Zveřejnění certifikátů a CRL	36
6.4.12.4	Zveřejňování informací o autoritě časového razítka	36
6.4.12.5	Periodicita zveřejňování informací	36
6.4.12.6	Řízení přístupu k jednotlivým typům úložišť	36
6.5	Ostatní obchodní a právní záležitosti	37
6.5.1	Poplatky	37
6.5.1.1	Poplatky za vydání kvalifikovaných elektronických časových razítek	37
6.5.1.2	Poplatky za přístup k certifikátu poskytovatele	37
6.5.1.3	Poplatky za informace o stavu certifikátu nebo o zneplatnění certifikátu poskytovatele	37
6.5.1.4	Poplatky za další služby	37
6.5.2	Finanční odpovědnost	37
6.5.2.1	Krytí pojištěním	37
6.5.2.2	Další aktiva a záruky	37
6.5.2.3	Pojištění nebo krytí zárukou pro koncové uživatele	37
6.5.3	Důvěrnost obchodních informací	38
6.5.3.1	Výčet důvěrných informací	38
6.5.3.2	Informace mimo rámec důvěrných informací	38
6.5.3.3	Odpovědnost za ochranu důvěrných informací	38
6.5.4	Ochrana osobních údajů	38
6.5.5	Práva duševního vlastnictví	38
6.5.6	Zastupování a záruky	38
6.5.6.1	Zastupování a záruky TSA	38
6.5.6.2	Zastupování a záruky třetí strany	39
6.5.6.3	Zastupování a záruky zákazníka, odpovědné osoby nebo žadatele	39
6.5.6.4	Zastupování a záruky ostatních zúčastněných subjektů	39
6.5.7	Zřeknutí se záruk	39
6.5.8	Omezení odpovědnosti	39
6.5.8.1	Odpovědnost zákazníka	39

6.5.8.2	Odpovědnost pověřených osob	39
6.5.8.3	Odpovědnost žadatele	40
6.5.8.4	Odpovědnost poskytovatele	40
6.5.9	Odpovědnost za škodu, náhrada škody	40
6.5.10	Doba platnosti, ukončení platnosti	40
6.5.10.1	Doba platnosti	40
6.5.10.2	Ukončení platnosti.....	40
6.5.10.3	Důsledky ukončení platnosti	41
6.5.11	Komunikace mezi zúčastněnými subjekty.....	41
6.5.11.1	Komunikace s poskytovatelem služby vydávání kvalifikovaných elektronických časových razítek	41
6.5.11.2	Komunikace v rámci ACAeID	41
6.5.11.3	Komunikační jazyk	41
6.5.12	Změny v CP	41
6.5.12.1	Postup při změnách	41
6.5.12.2	Postup při oznamování změn.....	41
6.5.12.3	Okolnosti, při kterých musí být změněno OID.....	41
6.5.13	Řešení sporů	42
6.5.14	Rozhodné právo	42
6.5.15	Shoda s právními předpisy	42
6.5.16	Další ustanovení	42
6.5.16.1	Vyšší moc	42
6.5.17	Další opatření	43
6.5.17.1	Použitá literatura a řídící dokumenty.....	43
6.5.17.2	Návazné dokumenty	43
7	Závěrečná ustanovení	44

1 ÚVOD

Tento dokument pro kvalifikovaná elektronická časová razítka obsahuje zásady a postupy související se zajištěním činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 a předpisů souvisejících.

Tento dokument stanovuje zásady, které PCS uplatňuje při zajišťování služeb vytvářejících důvěru:

- vydání kvalifikovaných elektronických časových razítek.

Pojem kvalifikované elektronické časové razítko je popsán v Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 a je jím datová zpráva, kterou vydal kvalifikovaný poskytovatel služeb vytvářejících důvěru, a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Certifikační politika TSA odpovídající Certifikační prováděcí směrnici TSA je určena žadatelům o poskytnutí výše vyjmenované služby, všem spoléhajícím se stranám a jiným účastníkům PKI.

Struktura tohoto dokumentu vychází ze struktury stanovené v příloze č. 2, z dokumentu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework a ČSN ETSI TS 102 023 v1.2.1 – Electronic Signatures and Infrastructures (ESI); Policy requirements for time stamping authorities. Tato Certifikační politika je v souladu s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

Informační systém ACAeID je budován a provozován ve shodě s právním prostředím České republiky.

Technické specifikace se řídí technickými normami ETSI EN 319 401, ETSI EN 319 411, ETSI EN 319 421, ETSI EN 319 422.

Společnost eIdentity a. s. provozuje novou hierarchickou strukturu certifikačních autorit, respektující stanoviska dozorového orgánu.

2 SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

2.1 Rejstřík zkratk

Zákon	Zákon 297/2016 Sb. o službách vytvářejících důvěru
ACAeID, ACA	Informační systém elidentity a.s., poskytující kvalifikované služby vytvářející důvěru
RCA	Kořenová certifikační autorita, jako součást ACAeID
QCA	Vydávající certifikační autorita, jako součást ACAeID
TSA	Autorita vydávající kvalifikovaná elektronická časová razítka
RM	Registrační místo
ORM	Operátor registračního místa
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
QC	Kvalifikovaný certifikát pro elektronický podpis
QSC	Kvalifikovaný certifikát pro elektronickou pečeť
QTS	Kvalifikované elektronické časové razítko
RQSC	Kořenový certifikát
CRL	Seznam zneplatněných certifikátů
PCS	Poskytovatel služeb vytvářejících důvěru
EVI	Evidenční část informačního systému PCS
CCTV	Uzavřené televizní okruhy (Closed Circuit Television)
EZS	Elektronické zabezpečovací systémy
EPS	Elektronická požární signalizace
DN	Distinguished Name – Jednoznačná identifikace subjektu certifikátu
UTC	Coordinated Universal Time - Světový koordinovaný čas, časový standard založený na Mezinárodním atomovém čase (TAI) s přestupnými sekundami
HSM	Hardware Security Module je zařízení pro bezpečné uložení klíčů a certifikátů, práce s tímto zařízením vyžaduje součinnost více osob
TSU	jednotka vydávající kvalifikovaná elektronická časová razítka jako součást TSA
TSA	autorita vydávající kvalifikovaná elektronická časová razítka. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a certifikát.
TST	Time Stamp Token – souhrnné označení dat tvořících časové razítko
Zákon znění Z300	Zákon č. 297/2016 Sb. o službách vytvářejících důvěru, v platném
FIPS	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů
Nařízení eIDAS	Federal Information Processing Standards, mezinárodně respektovaný standardizační orgán USA
	Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014

2.2 Rejstřík pojmů

Soukromý klíč	Data pro vytváření elektronických podpisů nebo pečeti
Veřejný klíč	Data pro ověřování elektronických podpisů nebo pečeti

Seznam použitých pojmů a zkratk



Revokace
Hash

zneplatnění certifikátu
Otisk, výtah či fingerprint je řetězec pevné délky, vzniklý z libovolně
dlouhého vstupního řetězce povolenou kryptografickou funkcí

3 ZÁKLADNÍ POJETÍ

Postupy, pravidla, technologie a ostatní skutečnosti popsané v tomto dokumentu dokladují důvěryhodnost a integritu řešení ACAeID při poskytování služeb vytvářejících důvěru, a to po celou dobu životního cyklu certifikátů či jiných produktů poskytovaných provozovatelem.

Informace o dalších provozovaných službách jsou popsány v jejich projektové dokumentaci, jejich Certifikačních politikách a na internetových stránkách provozovatele.

Ve veřejné části webového prostoru provozovatele jsou umístěny informace, které umožní zájemci či žadateli kvalifikovaně se rozhodnout o poskytovaných službách, svých povinnostech a právech. K dispozici mu je také odpovídající Certifikační politika a další dokumenty.

V informačním systému ACAeID jsou zpracovávány a uchovávány informace v souladu se zákonem 297/2016 Sb. a zákonem 101/2000 Sb. tak, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné. Zveřejňované informace jsou určeny zejména spoléhajícím se třetím stranám, aby bylo možné rozhodnout o platnosti certifikátu či kvalifikovaného elektronického časového razítka s požadovaným stupněm důvěry.

Každý žadatel o poskytnutí služby či podepisující osoba má přístup do svého účtu u provozovatele, kde má k dispozici seznam všech svých poskytnutých či právě poskytovaných služeb a může jejich stav sledovat a měnit v rozsahu své autorizace v systému.

3.1 Služby autority časových razítek (TSA)

Společnost eIdentity a.s. poskytuje služby autority časových razítek registrovaným uživatelům na základě jejich autorizace k využívání této služby. Služba je poskytnuta po jejich správné identifikaci a autentizaci.

Pro identifikaci a autentizaci lze využít komerčního či komerčního serverového certifikátu (a s využitím páru klíčů takovým certifikátům odpovídajícím), vydaného některou autoritou provozovanou společností eIdentity a.s. či jinou autoritou, kterou pro tento účel akceptuje společnost eIdentity a.s. v obchodní smlouvě. Smluvně lze domluvit i jiný akceptovatelný způsob identifikace a autentizace.

Podmínky poskytování služby kvalifikovaného elektronického časového razítka jsou dány tímto dokumentem a uzavřenou obchodní smlouvou.

3.2 Autorita časových razítek

Autorita časových razítek je složena z jedné či více jednotek, vydávajících časová razítka. Každá taková jednotka používá svoje data pro vytváření elektronické pečeti a svůj certifikát.

Každá taková jednotka je důvěryhodným způsobem navázána na UTC a pro určení času využívá správného měřidla času.

Distribuce času je řešena pomocí NTP protokolu. Primární server TSA, který přijímá požadavky klientů, je synchronizován s několika důvěryhodnými zdroji času. Tento server pak dále poskytuje čas TSU jednotkám a kontroluje, že časy a přesnost odpovědí TSU jsou v pořádku. V případě selhání kontrol není uživateli razítko poskytnuto.

Přímo v síti eidentity je umístěn přijímač, který je napojen na UTC čas pomocí GPS signálu a pracuje jako měřidlo času. Přístroj je vybaven doplňkovým oscilátorem, který udrží kvalitu času i po delší dobu případné poruchy GPS signálu. Tento přístroj je kalibrován přesně pro danou lokalitu a poskytuje pomocí NTP čas vnitřní síti. Server je umístěn společně s ostatní infrastrukturou eidentity a je tedy fyzicky dostatečně chráněn. Čas poskytuje pouze v rámci vnitřní sítě a není z Internetu dostupný.

Pro referenci jsou kromě tohoto vlastního zdroje času použity další dva NTP servery provozované nezávislými provozovateli. Pro zajištění důvěryhodnosti zdrojů času je ve všech případech použit protokol NTP v4 s autokey mechanismem, pomocí kterého je veškerá komunikace NTP ověřitelná.

Provozovatel autority časových razítek nese odpovědnost za kvalitu poskytovaných služeb kvalifikovaných elektronických časových razítek.

3.3 Zákazníci a odběratelé služby časového razítka

Zákazník je právnická nebo fyzická osoba či organizační složka státu, která má se společností eidentity a.s. uzavřen obchodní vztah. Zákazník ve smlouvě o poskytování služby sjedná způsob identifikace a autentizace ke službě kvalifikovaných elektronických časových razítek včetně určení míst, ze kterých bude služba odebírána a k nim odpovídající žadatele a sjedná případně i další parametry služby.

Žadatel je osoba určená ve smlouvě, která žádá o poskytnutí služby a jejímž jménem dochází i k odběru objednané služby.

Osoba oprávněná je taková určená osoba, která má právo jednat za zákazníka se společností eidentity a.s. v rozsahu ve smlouvě uvedeném.

3.4 Spoléhající se strany

Subjekty bez nutnosti vstupu do smluvního vztahu s poskytovatelem služby kvalifikovaného elektronického časového razítka a spoléhající se na kvalifikovaná elektronická časová razítka jsou spoléhající se strany.

4 POLITIKA TSA

4.1 Základní popis

Certifikační politika autority kvalifikovaných elektronických časových razítek popisuje životní cyklus časových razítek. Certifikační prováděcí směrnice autority kvalifikovaných elektronických časových razítek rozpracovává procesy a postupy vedoucí k zajištění životního cyklu kvalifikovaných elektronických časových razítek dle odpovídající Certifikační politiky.

Autoritu vydávající časová razítka elidentity a.s. tvoří kořenová autorita (RCA) a autorita vydávající kvalifikovaná elektronická časová razítka (TSA).

Autorita TSA se skládá z jedné či více jednotek (TSU), vydávajících kvalifikovaná elektronická časová razítka. Jednotkou, vydávající kvalifikovaná elektronická časová razítka je takový systém, který k žádosti o vystavení kvalifikovaného elektronického časového razítka vydá kvalifikované elektronické časové razítko obsahující důvěryhodný časový údaj.

Kořenová autorita RCA vydává certifikáty podřízeným certifikačním a časovým autoritám a vydala tedy i certifikát pro každou TSU časové autority vydávající kvalifikovaná elektronická časová razítka TSA.

Společnost elidentity a.s. provozuje i další certifikační autority, které se řídí svými Certifikačními politikami a provozními předpisy.

Spoléhající se stranou je každý subjekt, který využívá kvalifikovaných elektronických časových razítek vydaných ACAeID.

Další účastníci jsou orgány dozoru podle zákona 297/2016 Sb. a orgány činné v trestním řízení, případně další orgány, kterým to ze zákona přísluší.

4.2 Identifikace

Český normalizační institut přidělil společnosti elidentity a.s. OID ve tvaru 1.2.203.27112489.

Podtřída 1.2.203.27112489.1. je interně určena pro dokumentaci ACAeID, její další členění je určeno číslem dokumentu a jeho verzí, tedy např. 10.1.1.1 značí dokument ACAeID10.1 ve verzi 1.1.

Tato Certifikační politika – TSA má tyto identifikační znaky:

Identifikační znak	Význam identifikačního znaku	Hodnota
Název dokumentu	Název dokumentu v čitelné podobě	ACAeID10.4 Certifikační politika - TSA
OID	Identifikace dokumentu v rámci prostoru OID elidentity a.s.	1.2.203.27112489.1.10.4.1.1

4.3 Určení politiky a její použitelnosti

Jako přípustné použití kvalifikovaného elektronického časového razítka vydaného dle tohoto dokumentu

je takové použití, které je v souladu se zákonem č. 297/2016 Sb., Zákon č.300/2008 o elektronická a autorizované konverzi dokumentů nebo je v situacích, kdy je očekáván právně průkazný záznam existence konkrétních dat před daným časovým okamžikem.

4.4 Hodnocení shody a jiná hodnocení

V prostředí kvalifikovaného poskytovatele služeb vytvářejících důvěru jsou v souladu s požadavky legislativy i odborných či technických norem prováděny periodické i jednorázové prověrky shody provozovaného systému s určenými legislativními, bezpečnostními a technickými podmínkami. Hodnocení shody a audit systému probíhá v souladu s ISO9001.

4.4.1 Periodicita hodnocení

Pravidelně jedenkrát ročně je prováděn audit systému řízení bezpečnosti informací, eIdentity a.s. se musí na základě požadavků nařízení eIDAS jakožto kvalifikovaný poskytovatel služeb vytvářejících důvěru, alespoň jednou za 24 měsíců podrobit auditu ze strany akreditovaného subjektu posuzování shody. Výsledek musí dodat do 3 pracovních dnů dozorovému orgánu.

Společnost eIdentity a.s. si vyhrazuje právo k provádění i dalších kontrol, např. ohledně ochrany osobních údajů.

4.4.2 Identita a kvalita hodnotitele

Hodnocení shody a audity provádějí interní či externí hodnotitelé splňující požadavky odpovídající legislativy.

4.4.3 Vztah hodnotitele k hodnocené entitě

Interní hodnocení provádí interní auditor, který nemá jinou roli v hodnoceném systému.

Externí hodnocení provádí experti bez role v hodnoceném systému.

4.4.4 Hodnocené oblasti

Hodnocené oblasti jsou dány legislativou, která tato hodnocení předepisuje.

4.4.5 Postupy v případě zjištění nedostatků

Výsledky kontrol a případně zjištěné nedostatky jsou projednány na zasedání

Utajení: Veřejný dokument

Strana: 14

Bezpečnostního výboru, jehož členem je i zástupce vedení společnosti, nejčastěji

předseda představenstva. Bezpečnostní výbor určí i způsob vypořádání případných problémů a výsledek vypořádání projedná na některém dalším zasedání.

4.4.6 Sdělování výsledků hodnocení

Výsledek hodnocení či auditu je ve formě závěrečné zprávy předložen vedení společnosti a bezpečnostnímu řediteli na jednání Bezpečnostního výboru. Po projednání závěrečné zprávy a s ohledem na zachování bezpečnosti informací může výbor rozhodnout o jejím případném zveřejnění.

5 ZÁVAZKY A ODPOVĚDNOSTI

5.1 Závazky TSA

5.1.1 Obecné závazky TSA

Společnost eldentity a.s. jakožto provozovatel autority časového razítka ručí:

- že postupuje v souladu s platnou legislativou,
- že provozuje autoritu časového razítka v souladu s interní dokumentací,
- že provozuje autoritu časového razítka v souladu s požadavky a postupy dle tohoto dokumentu,
- za nepřetržitý přístup ke službám TSA s výjimkou plánovaných či neplánovaných časových přerušení (vzniklých např. v souvislosti se synchronizací času vlivem zavedení přestupné sekundy a podobně.),
- že využívání služeb bude řádně zpoplatněno dle odpovídající obchodní smlouvy s využitím sjednaného způsobu identifikace a autentizace odběratele,
- že vydá kvalifikované elektronické časové razítko neprodleně po obdržení platného, úplného a správného požadavku.

5.1.2 Závazky TSA ve vztahu k žadatelům o kvalifikované elektronické časové razítko a držitelům kvalifikovaných elektronických časových razítek

Společnost eldentity a.s. jakožto provozovatel autority časových razítek zejména zaručuje:

- že vydaná kvalifikovaná elektronická časová razítka mají obsah v souladu se zákonem č. 297/2016 Sb.,
- že uvedený časový údaj odpovídá hodnotě UTC v okamžiku vytváření kvalifikovaného elektronického časového razítka s přesností 1 sekunda a čas je získán z měřidla času navázaného na UTC,
- že využívá důvěryhodnou synchronizaci času s odchylkou času uvedeného ve vydaných kvalifikovaných elektronických časových razítkách nepřesahující 1 sekundu,
- data v elektronické podobě, která jsou předmětem žádosti o kvalifikované elektronické časové razítko a která jednoznačně odpovídají datům v elektronické podobě obsaženým ve vydaném kvalifikovaném elektronickém časovém razítku,
- že neověřuje předmět dat, který odpovídá datům v elektronické podobě obsaženým ve vydaném kvalifikovaném elektronickém časovém razítku,
- že vydaná odpověď na žádost o kvalifikované elektronické časové razítko obsahuje zejména:
 - číslo kvalifikovaného elektronického časového razítka,
 - identifikátor politiky, podle které bylo kvalifikované elektronické časové razítko vydáno,
 - obchodní firmu a stát, ve kterém je kvalifikovaný poskytovatel usazen,
 - hodnotu času v UTC, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného elektronického časového razítka s přesností 1 sekunda,
 - data v elektronické podobě, pro která bylo kvalifikované elektronické časové razítko vydáno,
 - elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru (TSU), který kvalifikované elektronické časové razítko vydal.

5.2 Závazky žadatelů o kvalifikované elektronické časové razítko a držitelů kvalifikovaného elektronického časového razítka

Žadatel či držitel zkontroluje po obdržení odpovědi na žádost o kvalifikované elektronické časové razítko informaci o stavu zpracování této žádosti.

V případě, že kvalifikované elektronické časové razítko bylo vydáno, provede dále tyto činnosti:

- ověří platnost elektronické pečeti pomocí certifikátu vydávající TSU,
- ověří platnost elektronických pečeti celého příslušného certifikačního řetězce,
- ověří, zda OID politiky pro vydávání kvalifikovaných elektronických časových razítek, které je uvedeno v odpovědi, odpovídá OID uvedenému v tomto dokumentu,
- v případě, že žádost obsahovala položku „nonce“ nebo/a položku „reqPolicy“, ověří, že její hodnota v odpovědi je shodná.

Zákazník dále ručí za naplnění všech svých povinností dle tohoto dokumentu i dle zákona č. 297/2016 Sb. a návazných předpisů.

5.3 Závazky spoléhajících se stran

Spoléhající se strana ověřuje obsah časového razítka:

- otisk (hash) ověřovaných dat,
- platnost elektronické pečeti pomocí certifikátu TSU.

Spoléhající se strana získá bezpečným způsobem aktuální příslušná CRL a ověří platnost:

- elektronické pečeti pomocí certifikátu vydávající TSU,
- elektronických pečeti celého příslušného certifikačního řetězce.

Spoléhající se strana zvaží, zda kvalifikované elektronické časové razítko vydané podle této politiky, je vhodné pro účel, ke kterému bylo použito.

Spoléhající se strana ověří, zda jsou kryptografické funkce použité v časovém razítku stále platné a bezpečné, jedná se zejména o:

- kryptografickou funkci pro tvorbu hashe,
- kryptografický algoritmus použitý při označování razítka,
- délku klíče u kryptografického algoritmu použitého pro označení razítka.

5.4 Odpovědnost

Společnost eIdentity a.s. neodpovídá za vady poskytovaných služeb a škody vzniklé z důvodů nesprávného použití či porušením povinností vyplývajících z tohoto dokumentu či jiných legislativních předpisů.

Společnost eIdentity a.s. neodpovídá za vady vzniklé z důvodu vyšší moci včetně výpadků telekomunikačního spojení.

Závazky a odpovědnosti



Tato ustanovení zůstávají v platnosti i po ukončení platnosti tohoto dokumentu.

6 POŽADAVKY NA POSTUPY A PROCESY TSA

6.1 Správa politiky

6.1.1 Organizace spravující politiku a prováděcí směrnici TSA

eIdentity a.s.
Vinohradská 184/2396
130 00 Praha 3
Česká republika

IČ: 271 12 489
DIČ: CZ27112489

Společnost je zapsána v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 9080.

6.1.2 Kontaktní osoba spravující tento dokument

Za správu tohoto dokumentu odpovídá předseda Výboru pro politiky.

Soulad Certifikační politiky s jí odpovídající Certifikační prováděcí směrnici schvaluje Výbor pro politiky na základě schůze Výboru a v souladu s jednacím řádem tohoto orgánu.

Kontaktní údaje zodpovědné osoby:

Předseda Výboru pro politiky
eIdentity a.s.
Vinohradská 184
130 00 Praha 3
Česká republika

Tel: +420 222 866 150
Fax: +420 222 866 159
Email: PAA-manager@eidentity.cz

6.1.3 Postupy při schvalování tohoto dokumentu

Tento dokument je na zasedání Výboru pro politiky projednán a schválen. Postup schvalování je určen jednacím řádem Výboru pro politiky.

6.2 Požadavky na životní cyklus párových dat TSA

6.2.1 Generování a instalace párových dat

6.2.1.1 Generování párových dat

Generování párových dat probíhá v zabezpečené zóně v souladu s interní dokumentací. O průběhu generování párových dat je vyhotoven písemný protokol. Data jsou generována do kryptografického modulu, který splňuje požadavky Nařízení eIDAS a technické normy.

6.2.1.2 Vlastnosti kryptografického modulu

Kryptografický modul použitý pro generování a úschovu soukromých klíčů TSA (bezpečný kryptografický modul) splňuje požadavky standardu FIPS 140–2 Level 3 a vyšší.

6.2.1.3 Poskytování veřejných klíčů

Veřejné klíče, sloužící pro ověřování elektronických pečeti vydávaných časových razítek, jsou obsažena v certifikátu TSU. Tento certifikát je možno získat nejméně dvěma nezávislými kanály:

- prostřednictvím internetových stránek eidentity a.s.,
- prostřednictvím internetových stránek ministerstva,
- ve Věstníku ministerstva.

6.2.1.4 Délky párových dat

TSA používá pro vytváření elektronických pečeti asymetrický kryptografický algoritmus RSA. Mohutnost klíčů (modulů) použitých pro pečetění vydávaných časových razítek je 2048 bitů.

6.2.2 Ochrana soukromého klíče TSA (dat pro vytváření elektronických pečeti)

6.2.2.1 Standardy a podmínky používání kryptografického modulu

Soukromé klíče, sloužící pro vytváření elektronických pečeti vydávaných časových razítek, jsou uloženy v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 úroveň 3 a platné legislativy.

6.2.2.2 Zálohování soukromých klíčů

Soukromé klíče jsou chráněny kryptografickým modulem, který umožňuje jejich obnovu za pomoci přinejmenším tří z pěti administrátorských karet, vytvořených při instalaci a zálohy klíčových dat dle dokumentace modulu.

6.2.2.3 Uchovávání soukromých klíčů

Soukromé klíče jsou uchovávány jen v provozním prostředí modulu a/nebo v záloze klíčových dat. V záloze se soukromé klíče nevyskytují v otevřené formě, ale jsou chráněny administrátorským cardsetem dle specifikace výrobce a dle dokumentace modulu.

6.2.2.4 Transfer soukromých klíčů

Soukromé klíče TSA jsou uchovávány v kryptografickém modulu a veškeré operace s těmito klíči jsou prováděny výhradně v tomto modulu.

6.2.2.5 Uložení soukromých klíčů v kryptografickém modulu

Soukromé klíče TSA jsou uloženy v aktivovaném a nakonfigurovaném kryptografickém modulu.

6.2.2.6 Aktivační data

Aktivační data jsou uložena v bezpečnostním tokenu každého člena obsluhy a jsou chráněna osobním PIN kódem, který si dotyčný zvolil při instalaci.

6.2.2.7 Postup při aktivaci soukromých klíčů

Soukromé klíče jsou aktivovány obsluhou dle dokumentace kryptografického modulu. K aktivaci stačí jedna osoba s kartou z operátorského cardsetu.

6.2.2.8 Postup při deaktivaci soukromých klíčů

K deaktivaci soukromých klíčů postačuje jedna osoba v roli Administrátora TSU. Klíče jsou též deaktivovány automaticky v rámci procesu vypnutí systému.

6.2.2.9 Postup při zničení soukromých klíčů

Soukromé klíče, které jsou uchovávány v HSM, jsou zničeny pomocí prostředků tohoto HSM. Současně jsou zničeny i jejich zálohy. Ničení soukromého klíče zahrnuje i ničení karet z operátorského cardsetu, které jsou nezbytné k aktivaci těchto klíčů. K ničení dojde na základě rozhodnutí Bezpečnostního výboru nebo vedení společnosti.

6.2.3 Distribuce veřejných klíčů

Veřejné klíče jednotlivých TSU jsou k dispozici na stránkách eIdentity a.s. a ministerstva.

6.2.4 Žádost o certifikáty TSA

Každá jednotka TSU vytvoří žádost ve formátu PKCS#10, na základě které kořenová

certifikační autorita vydá certifikát v souladu s provozní dokumentací.

6.2.4.1 Profil certifikátu

Položka	Obsah
Version	verze 3
Serial Number	jedinečné číslo vydaného certifikátu
SignatureAlgorithm	identifikátor algoritmu, použitého elidentity pro elektronickou pečeť certifikátu vydaného konkrétnímu TSU (sha256WithRSAEncryption)
Issuer	označení vydavatele certifikátu
Validity	počátek konec platnosti certifikátu
Subject	označení držitele certifikátu
SubjectPublicKeyInfo	identifikátor algoritmu využívaný veřejným klíčem uvedeným ve vydávaném certifikátu a veřejný klíč vydávaného certifikátu (2048bitů)
Extensions	Rozšíření certifikátu

Jako Subject certifikátu se použije označení dle následující tabulky:

Položka	Obsah
Organization (O)	elidentity a.s.
OrganizationIdentifier	„VATCZ-27112489”
OrganizationUnitName(OU)	TSA3
CommonName (CN)	TSU3.n
Country (C)	CZ

Za proměnnou n se dosadí pořadové číslo jednotky časové autority. Číslování proměnné n začíná číslem 1 a jedná se o celá čísla.

6.2.5 Výměna párových dat

Doba platnosti certifikátů TSU je dle politiky kořenové certifikační autority maximálně 7 let. Výměna klíčů probíhá vydáním nového certifikátu kořenovou certifikační autoritou podle platné certifikační politiky a zneplatněním původního certifikátu s uvedením důvodu superseded (4). Klíče původního certifikátu jsou ničeny v souladu s kapitolou 6.2.2.9.

Z důvodu zajištění bezproblémového přechodu na nové TSU může zůstat certifikát původní TSU v platnosti i tehdy, když původní TSU již kvalifikovaná elektronická časová razítka nevydává a služby poskytuje už jen nové TSU.

6.2.6 Ukončení životního cyklu párových dat

Životní cyklus párových dat je ukončen zneplatněním certifikátu TSU s uvedením důvodu cessationOfOperation (5). Klíče certifikátu jsou ničeny v souladu s kapitolou 6.2.2.9.

6.2.6.1 Zneplatnění a pozastavení platnosti certifikátu

Informace o zneplatnění certifikátu je uvedena v seznamu zneplatněných certifikátu kořenové certifikační autority.

Certifikát TSU může být zneplatněn na základě následujících okolností:

- nastanou-li skutečnosti uvedené v Zákon
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci dat pro vytváření elektronických značek TSU.

6.2.7 Správa kryptografického modulu používaného při vytváření kvalifikovaných elektronických časových razítek

Proces akvizice kryptografického modulu probíhá v souladu s interní dokumentací a při instalaci jsou nastaveny požadované bezpečnostní parametry dle pokynů výrobce.

6.2.7.1 Hodnocení kryptografického modulu

Kryptografický modul sloužící pro vydávání časových razítek odpovídá požadavkům na kryptografické moduly dle dokumentu „Standard pro hodnocení bezpečnosti kryptografických modulů“ vydaný NIST v USA – FIPS PUB 140-2, úroveň 3“ a byla mu vyslovena shoda s požadavky

6.3 Vydávání kvalifikovaných elektronických časových razítek

6.3.1 Uzavření smlouvy a registrační proces

Pro využívání služby kvalifikovaných elektronických časových razítek je nutné nejdříve uzavřít Smlouvu. Smlouvu je možné uzavřít v listinné podobě či v elektronické podobě. Obě podoby mají stejný právní význam.

Mimo obchodních podmínek poskytování služby kvalifikovaného elektronického časového razítka je obsahem smlouvy i určení způsobu identifikace a autentizace žadající entity a případně je ve smlouvě uvedena i osoba pověřená a zodpovědná ve věcech souvisejících s plněním této smlouvy.

6.3.2 Zpracování žádosti o kvalifikované elektronické časové razítko

6.3.2.1 Identifikace a autentizace

Jako možné způsoby identifikace a autentizace je možné použít komerční nebo komerční serverový certifikát vydaný některou certifikační autoritou společnosti eIdentity a.s. nebo je možné smluvně sjednat jiný způsob identifikace a autentizace.

V případě úspěšné identifikace a autentizace získá žadatel jemu odpovídající autorizaci k poskytované službě.

6.3.2.2 Přijetí nebo zamítnutí žádosti o kvalifikované elektronické časové razítko

Úspěšně autorizovaný žadatel požádá o vydání kvalifikovaného elektronického časového razítka prostřednictvím klientské aplikace, která je zodpovědná za řádné sestavení žádosti včetně volby správného hashovacího algoritmu v souladu s normou RFC3161 a s dokumentem ETSI TS 102 176-1, resp. jejich případnými novelizacemi.

Komunikace s časovou autoritou probíhá zabezpečeným protokolem (např. SSL/TLS).

Žádost o službu je zamítnuta zejména v případě neúspěšné autorizace ke službě, nebo pokud žádost nesplňuje náležitosti určené v tomto dokumentu. Žádost o službu může být zamítnuta i z jiných důvodů, např. při porušení smluvních podmínek.

6.3.2.3 Doba zpracování žádosti o kvalifikované elektronické časové razítko

Kvalifikované elektronické časové razítko je vytvořeno po přijetí platné žádosti bez prodlení. Z pohledu žadatele však dojde k uplynutí určité doby od jeho pokynu k vytvoření žádosti o kvalifikované elektronické časové razítko do času, který je v razítku uveden. V této době se ze zprávy či dokumentu v elektronické formě vytváří otisk za pomoci zvoleného algoritmu, sestaví se vlastní žádost a (po předchozí identifikaci a autentizaci) se zašle do TSA. Délka této doby závisí zejména na velikosti zpracovávaného souboru, kvalitě použitého algoritmu pro otisk nebo aktuálních parametrech transportní cesty od žadatele k TSA a jejím TSU.

6.3.3 Vydání kvalifikovaného elektronického časového razítka

6.3.3.1 Úkony TSA v průběhu vydávání kvalifikovaného elektronického časového razítka

Systém TSA provede kontrolu správnosti žádosti o kvalifikované elektronické časové razítko a v případě kladného výsledku vytvoří odpověď podle RFC3161, která obsahuje kvalifikované elektronické časové razítko. Časový údaj, uvedený v kvalifikovaném elektronickém časovém razítku odpovídá okamžiku vytvoření tohoto časového razítka. Časový údaj poskytuje řádně kalibrované měřidlo času, které je bezpečným způsobem navázáno na UTC a je porovnáváno s dalšími nezávislými zdroji informace o času. Odchylka měřidla času nepřesahuje 1 sekundu a je neustále sledována. Pokud by vlivem nějaké události nebylo možné toleranci udržet, kvalifikované elektronické časové razítko se nevydává.

Kvalifikované elektronické časové razítko může obsahovat i další informace, zejména o měřidle času.

Kvalifikované elektronické časové razítko je opatřeno elektronickou značnou jednotky

TSU, která razítko vydala. Vyrobená kvalifikovaná elektronická časová razítka jsou

archivována dle interní dokumentace po dobu nejméně 10 let.

6.3.3.2 Oznámení o vydání kvalifikovaného elektronického časového razítka žadateli o vydání kvalifikovaného elektronického časového razítka

Požadavky na postupy a procesy TSA



V případě vydání časového razítka je toto razítko odesláno žadateli. V případě neposkytnutí služby je žadateli tato informace vrácena včetně případných doplňujících informací dle RFC3161.

6.3.3.3 Převzetí kvalifikovaného elektronického časového razítka

Žadatel o kvalifikované elektronické časové razítko je po přijetí zprávy od TSA povinen zjistit status odpovědi. Pokud odpověď též obsahuje kvalifikované elektronické časové razítko, může ho akceptovat až po splnění povinnosti dle bodu 5.2 tohoto dokumentu.

6.3.4 Ověření kvalifikovaného elektronického časového razítka

Při ověřování kvalifikovaného elektronického časového razítka je potřeba ověřit jednak vlastní obsah časového razítka a dále také ověřit platnost elektronické pečeti, kterou je razítko opatřeno.

Pro ověření obsahu kvalifikovaného elektronického časového razítka je potřeba:

- ověřit, zda čas, který je v razítku uveden, odpovídá přibližně času, kdy byla žádost připravována,
- ověřit, zda otisk dat uvedený v razítku odpovídá otisku dat vypočtených na straně Žadatele,
- ověřit, zda je zachována integrita časového razítka.

Pro ověření elektronické pečeti, kterou je kvalifikované elektronické časové razítko opatřeno, je potřeba:

- získat aktuálně platný seznam zneplatněných certifikátů (CRL) autority, která vydala certifikát zkoumané TSU,
- zkontrolovat integritu tohoto seznamu CRL,
- zkontrolovat, zda v něm není uveden certifikát TSU,
- a podobně postupovat až k certifikátu kořenové autority ve zkoumaném certifikačním řetězci.

V případě, že otisky dat jsou při shodném algoritmu shodné a byla ověřena platnost všech elektronických pečeti a certifikátů, je kvalifikované elektronické časové razítko platné.

6.3.5 Platnost kvalifikovaného elektronického časového razítka

Stav kvalifikovaného elektronického časového razítka závisí také na stavu certifikátu TSU, který je používán pro ověření elektronické pečeti na časovém razítku.

Pravidla pro určení platnosti časového razítka ve vazbě na stav certifikátu TSU určuje RFC3161 a jsou následující:

Pokud je certifikát TSU platný, je kvalifikované elektronické časové razítko platné.

Pokud je certifikát TSU platný vzhledem k uvedené době platnosti v certifikátu a byl zneplatněn s následujícími důvody zneplatnění:

- unspecified (0),
- affiliationChanged (3),
- superseded (4), nebo
- cessationOfOperation (5),

je kvalifikované elektronické časové razítko, které bylo vydáno před časem zneplatnění

certifikátu, platné.

Kvalifikované elektronické časové razítko, které bylo vydáno po čase zneplatnění certifikátu TSU z výše uvedených důvodů, je neplatné.

Pokud byl certifikát TSU zneplatněn s následujícími důvody zneplatnění:

- keyCompromise (1),
- caCompromise (2),
- důvod zneplatnění není uveden,

je kvalifikované elektronické časové razítko od času jeho vytvoření neplatné.

Pokud platnost certifikátu TSU vypršela a tento certifikát nebyl zneplatněn, není standardními kontrolami možné ověřit platnost časového razítka. V takovém případě je podle potřeb spoléhající se strany nezbytné použít dodatečná opatření, kterými mohou být například:

- požádat o nové kvalifikované elektronické časové razítko,
- autorizovaná konverze dokumentu s časovým razítkem do papírové formy,
- uložení elektronické formy dokumentu s časovým razítkem na nepřepisovatelné medium nebo do archivu s podobnou funkcí,
- použít nadstandardní kontroly dle ČSN ETSI TS 102 023.

6.3.6 Struktura žádosti, odpovědi a kvalifikovaného elektronického časového razítka

6.3.6.1 Struktura žádosti o kvalifikované elektronické časové razítko

Položka		Popis	Hodnota
Version		Verze protokolu časového razítka (povinná položka)	1
messageImprint	HashAlgorithm	OID hash algoritmu (povinná položka)	SHA-256, SHA-384, SHA-512
	HashedMessage	Otisk dat (povinná položka)	
reqPolicy		Identifikátor politiky (nepovinná položka)	1.2.203.27112489.1.10.4.1.1
nonce		Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	
certReq		TRUE – odpověď musí obsahovat certifikát TSU FALSE nebo nevyplněno – odpověď nesmí obsahovat certifikát TSU (nepovinná položka)	TRUE, FALSE
extensions		Žádná rozšíření nejsou povolena	

Žadosti, které využívají otisku dat (hashe) podle algoritmu SHA1, nemusí být od 1. 1. 2011 přijímány.

6.3.6.2 Struktura odpovědi na žádost o kvalifikované elektronické časové razítko

Položka	Popis	Hodnota
PKIStatus	Přirozené číslo, označující stav odpovědi (přidělení nebo nepřidělení časového razítka). Kvalifikované elektronické časové razítko bylo přiděleno a je součástí odpovědi, pouze pokud je hodnota tohoto pole 0 nebo 1.	0 – TST bylo vydáno 1 – TST bylo vydáno (upravené) 2 – odmítnutí žádosti 3 – čekání na odpověď 4 – bezprostřední zneplatnění certifikátu TSU 5 – certifikát byl zneplatněn
PKIFailureInfo	BIT STRING. Uvádí důvod nepřidělení časového razítka. Součástí odpovědi na žádost o kvalifikované elektronické časové razítko je pouze v případě, že hodnota pole PKIStatus je jiná než 0 nebo 1 a kvalifikované elektronické časové razítko tedy není v odpovědi přítomno.	BadAlg – neznámý nebo nepodporovaný algoritmus BadRequest – nepovolená nebo nepodporovaná transakce BadDataFormat – špatný formát zaslaných dat TimeNotAvailable – nedostupný zdroj času TSA UnacceptedPolicy – požadovaná politika není podporovaná ze strany TSA UnacceptedExtension – požadované rozšíření není podporované ze strany TSA AddInfoNotAvailable – požadované doplňující informace nebyly identifikované nebo nejsou dostupné SystemFailure – žádost nemohla být zpracována kvůli chybě systému

6.3.6.3 Struktura kvalifikovaného elektronického časového razítka

Položka		Popis	Hodnota
Version		Verze protokolu časového razítka	1
Policy		Identifikátor politiky	1.2.203.27112489.1.10.4.1.1
messageImprint	HashAlgorithm	OID hash algoritmu	SHA-256, SHA-384, SHA-512
	HashedMessage	Otisk dat	
serialNumber		Přirozené číslo do 160 bitů.	TSU přiděluje každému časovému razítku unikátní číslo
genTime		GeneralizedTime – hodnota UTC	
accuracy		Aktuální přesnost časové informace	
ordering		Položka definující vztah dvou časových razítek	FALSE
nonce		Náhodné, jednou vygenerované číslo (64 bitů). Je-li obsaženo v žádosti, pak ho obsahuje i odpověď. (nepovinná položka)	
TSA		Rozlišovací jméno TSU	

TSA vloží do každého časového razítka údaj, který jednoznačně určuje politiku, podle níž bylo razítko vydáno.

Poskytovatel služby vydávání časových razítek zajišťuje, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného elektronického časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném elektronickém časovém razítku.

TSU vloží do každého nově generovaného časového razítka celé číslo, jehož hodnota je jedinečná – položka serialNumber. Sériové číslo umístěné v časovém razítku je pro každé TSU v rámci TSA jednoznačné. Jednoznačnost v rámci TSA a poskytovatele certifikačních služeb je zajištěna kombinací položek časového razítka serialNumber a TSA.

TSA vloží do každého časového razítka důvěryhodnou hodnotu času, která odpovídá hodnotě UTC v čase přidělení časového razítka. Pole genTime časového razítka uvádí čas, kdy kvalifikované elektronické časové razítko bylo vytvořeno autoritou časových razítek.

6.3.7 Synchronizace měřidla času s UTC

6.3.7.1 Synchronizace

V systémech TSA je využíváno měřidlo času, které je navázáno na světový koordinovaný čas. V pravidelných intervalech je synchronizováno se zdrojem UTC času, konkrétně UTC(USNO), pomocí technologie GPS. Návaznost času poskytovaného měřidlem času na

UTC je prokázána úředním kalibračním měřením. Písemný záznam o kalibračním měření, o elektrické délce anténního svodu a o zpoždění na výstupu NTP je uložen v sídle společnosti eidentity a.s. Čas získaný z těchto měřidel je dále uvnitř systémů TSA distribuován (probíhá synchronizace času) pomocí protokolu NTP v4. Problematika synchronizace je podrobně řešena interní dokumentací TSA.

6.3.7.2 Bezpečnost měřidla času

Měřidlo času je umístěno v zabezpečených prostorách v souladu s interní dokumentací.

6.3.7.3 Detekce odchýlení měřidla času

Jako kontrolní zdroj času jsou použity 2 externí NTP servery, které jsou přímo navázány na zdroj UTC, na který je navázán i státní etalon času. Stav měřidel času a jejich časová odchylka se kontroluje v pravidelných intervalech jedenkrát za dva roky.

Pokud by vlivem nějaké situace nebylo možné toleranci udržet, kvalifikované elektronické časové razítko se nevydává.

6.3.7.4 Přestupná sekunda

Systém TSA je s UTC synchronizován včetně výskytu přestupné sekundy v souladu s interní dokumentací.

Kvalifikované elektronické časové razítko se nevydává po nezbytně dlouhou dobu před zavedením přestupné sekundy, po dobu zavádění přestupné sekundy a po nezbytně dlouhou dobu po zavedení přestupné sekundy. Uvedené nezbytně dlouhé doby slouží ke správnému zavedení přestupné sekundy, k synchronizaci času měřidel času a ke kontrole provedení zavedení přestupné sekundy. O technologických odstávkách v souvislosti s přestupnou sekundou či v souvislosti s jinými profylaktickými pracemi je veřejnost informována na webových stránkách eidentity a.s.

6.4 Správa a provozní bezpečnost TSA

6.4.1 Řízení bezpečnosti

Řízení bezpečnosti je zavedeno dle normy ČSN ISO 27001 a posuzování shody probíhá formou auditu či formou částečného posouzení shody v intervalech určených platnou legislativou.

6.4.2 Hodnocení a řízení rizik

Hodnocení a řízení rizik je určeno vnitřní dokumentací.

6.4.3 Personální bezpečnost

Společnost eidentity a.s. při práci s lidskými zdroji vybudovala systém, který zabezpečuje,

že budou najímáni pouze důvěryhodní zaměstnanci a je dbáno o to, aby jejich loajalita ke společnosti byla podporována a udržována. Personální práce elidentity a.s. vede k tomu, že lidé si uvědomují zájem společnosti o ně samé, že cítí sounáležitost se svou společností, identifikují se s ní a cítí jasnou přímou úměrnost mezi úspěchem společnosti a svým prospěchem. Pro společnost je základním východiskem důvěra ve vlastní zaměstnance, která má pozitivní vliv na míru akceptování některých omezení. Personální bezpečnost je součástí aktivit spadajících pod řízení lidských zdrojů, je tedy neoddelitelnou součástí práce všech vedoucích pracovníků elidentity a.s. Personální bezpečnost elidentity a.s. vnímá jako součást řádné správy společnosti, neboť je vyjádřením péče o svěřená aktiva.

Personální bezpečnost v oblasti ochrany citlivých aktiv tedy elidentity a.s. vnímá jako zintenzivnění výše uvedeného systému u osob, které jsou určeny k práci s citlivými aktivy. Organicky navazuje na současný systém řízení lidských zdrojů.

Termínem personální bezpečnost elidentity a.s. označuje souhrn všech postupů, které vedou k ověření důvěryhodnosti zaměstnanců a k jejich vzdělávání vedoucím k bezpečnostnímu povědomí o možných bezpečnostních hrozbách a rizicích a k jednání, která toto povědomí odráží.

Důvěryhodnost zaměstnanců je jedním ze základních kvalifikačních předpokladů pro výkon pracovní činnosti v rámci elidentity a.s. Je zárukou toho, že pracovník, který disponuje svěřenými hodnotami, svého postavení nezneužije a nezpůsobí tak poskytovateli ztrátu.

Ověření důvěryhodnosti zaměstnance je proces zahrnující shromažďování, ověřování a vyhodnocování informací. Výstupem je rozhodnutí, zda může být daný jmenovaný pracovník (pracovník usilující o jmenování) považován za důvěryhodnou osobu.

Společnost elidentity a.s. má přijat propracovaný systém personální bezpečnosti. Jsou určeny bezpečnostní požadavky na zaměstnance i na průběh jejich přijímání. Součástí systému personální bezpečnosti jsou i postupy a plánování získávacích a udržovacích školení zaměstnanců dle hlediska jimi zastávané role i z hlediska obecné bezpečnosti informací.

Přesné postupy a pravidla jsou popsány v interní dokumentaci.

6.4.3.1 Důvěryhodné role

Seznam důvěryhodných rolí je obsahem interní dokumentace.

6.4.3.2 Role vyžadující rozdělení pravomocí

Matice rozdělení rolí je součástí interní dokumentace.

6.4.3.3 Požadavky na personál

Všichni pracovníci musí splnit požadavky na kvalitu osob a zastávají jen takové role, které nejsou v rozporu s maticí rozdělení rolí. Každý pracovník protokolárně projde získávacím školením a pak absolvuje pravidelné udržovací školení. Přesná pravidla školení určuje

interní dokumentace.

6.4.3.4 Požadavky na nezávislé dodavatele

Na pracovníky smluvních partnerů jsou kladeny stejné požadavky jako na vlastní zaměstnance.

6.4.3.5 Dokumentace poskytovaná zaměstnancům

Zaměstnanci disponují provozními a pracovními příručkami, které odpovídají jimi zastávaným rolím.

6.4.4 Fyzická bezpečnost a bezpečnost prostředí

6.4.4.1 Umístění a konstrukce

Podepisovací pracoviště s kryptografickým modulem a zařízení obsahující a zpracovávající osobní údaje žadatelů je umístěno ve vhodných geograficky vzdálených hlavních a záložních lokalitách. Použité prostory odpovídají svým bezpečnostním vybavením a režimem provozu objektům kategorie „D“ vyžadované zákonem 297/2016

Sb., pro umístění takových zařízení.

6.4.4.2 Fyzický přístup

Vstup do budovy, včetně do objektu, je pro vstupující možný při prokázání se identifikačním průkazem s fotografií strážní služby a současně při použití čipové karty (otočné turnikety ve vstupní hale). Vstupní dveře do ulice otevírá dálkově pouze strážní služba.

Návštěvy jsou v budově možné pouze s doprovodem zaměstnance po ověření totožnosti nebo samostatně osobám vybavených identifikační kartou.

Čipy je dále řešen vstup do jednotlivých částí komplexu (bez souvislosti s ochranou citlivých aktiv). Turnikety ve vstupní hale jsou nejúčinnějším prostředkem pro řízení pohybu. Dále je instalován systém CCTV, který chrání perimetr budovy a vybrané části prostor PCS.

Bezpečnost je dále v celém prostoru posílena o systém EZS a EPS s vyvedeným výstupem hlášení na stanoviště strážní služby.

6.4.4.3 Elektřina a klimatizace

Použité prostory jsou vybaveny nezávislým přívodem elektrické energie, záložním zdrojem elektrické energie a generátorem elektrické energie pro zachování napájení objektu elektrickou energií při dlouhodobém výpadku hlavních přívodů.

Prostory jsou klimatizovány a vlhkost je udržována automaticky.

6.4.4.4 Vliv vody

V používaných prostorech je odstraněno nebezpečí zalití vodou, místnosti jsou bez oken a bez rozvodu vody.

6.4.4.5 Protipožární opatření a ochrana

V případě požáru se použité místnosti naplní netečným plynem, který uhasí požár. Po odvětrání jsou prostory opět přístupné.

6.4.4.6 Ukládání médií

Média s provozními zálohami dat a systému jsou ukládány na dvou geograficky vzdálených místech v trezorech. Přístup k nim je řízen a kontrolován. O pohybu záložních médií je pořizován zápis.

6.4.4.7 Nakládání s odpady

Při provozu ACAeID nevznikají jiné než běžné odpady pro kancelářský režim práce. Tyto odpady se likvidují v souladu se zásadami nakládání s odpady.

6.4.4.8 Zálohy mimo budovu provozního prostředí

Pro zajištění schopnosti dodržet požadované termíny činností ACAeID jsou využity geograficky vzdálené prostory, které umožní v dostatečně krátké době znovu zprovoznit havarovaný nebo jinak nedostupný informační systém.

6.4.5 Řízení provozu

6.4.5.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejná část systému ACA eidentity je přístupná pomocí HTTP a HTTPS protokolu. Všechny komponenty veřejné části kromě registrace nových uživatelů jsou určeny pouze ke čtení a neumožňují vzdálenému uživateli změnu údajů. Registrace uživatelů vyžaduje vstup ze strany zájemce a je vedena striktně pomocí HTTPS protokolu.

Klientská část systému TSA je zpřístupněna uživatelům šifrovaným kanálem, kterým jsou předávána veškerá citlivá data. Přístup k údajům uživatele je umožněn až po zadání uživatelského jména a hesla. Toto rozhraní je jediným bodem komunikace s veřejností, všechny ostatní systémy TSA eidentity jsou mimo vnitřní síť CA eidentity nepřístupné.

Systémy ACAeID jsou od internetového provozu odděleny vhodným bezpečnostním zařízením (např. firewall) a přístupný provoz je řízen a kontrolován.

Systémy ACAeID jsou fyzicky umístěny v chráněném objektu typu „D“ a přístup k nim mají

pouze určené osoby.

6.4.5.2 Hodnocení počítačové bezpečnosti

Hodnocení vychází z níže uvedených norem a soulad s těmito normami je ověřen auditem:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů,
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty,
- ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pro management bezpečnosti informací,
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky,
- ČSN ISO/IEC TR 13335 - Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3,
- ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.
- ETSI EN 319 401, ETSI EN 319 411, ETSI EN 319 421, ETSI EN 319 422.

6.4.6 Řízení přístupu do systému

Přístup do systému TSA je řízen. Autorizace probíhá po úspěšné identifikaci a autentizaci a nastavení přístupových práv odpovídá roli, kterou uživatel získal.

6.4.7 Vývoj a údržba důvěryhodných systémů

6.4.7.1 Řízení vývoje systému

Vývoj systému probíhá podle pravidel zabezpečení vývoje v souladu s interní dokumentací.

6.4.7.2 Kontroly řízení bezpečnosti

Řízení bezpečnosti probíhá v uzavřeném cyklu:

- analýza požadavků a definice systému,
- návrh a řešení systému,
- integrace,
- implementace,
- provoz (užívání),
- nepřetržité hodnocení provozu,
- nepřetržité školení uživatelů.

6.4.8 Obnova po havárii nebo kompromitaci

6.4.8.1 Postup v případě havárie nebo kompromitace

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s plánem pro zvládání krizových situací a plánem obnovy.

6.4.8.2 Poškození výpočetních prostředků, software nebo dat

Systém je navržen tak, že je možné vyměnit jakoukoliv část poškozené výpočetní techniky, software a dat tak, aby mohl být provoz zachován či obnoven v požadovaném termínu.

6.4.8.3 Postup při zjištění odchýlení měřidla času

Při zjištění odchýlení měřidla času se po dobu nezbytně nutnou přerušuje vydávání kvalifikovaných elektronických časových razítek. Nezbytně nutná doba se využije k zjištění příčiny odchýlení, odstranění případné poruchy, k nové synchronizaci času v systému TSA a k opětovnému spuštění služby kvalifikovaného elektronického časového razítka.

Po následném projednání incidentu v Bezpečnostním výboru se navrhnou, implementují a posléze zhodnotí zvolená opatření k nápravě.

6.4.8.4 Kompromitace soukromého klíče TSA

V případě vzniku události, která má vliv na bezpečnost vydání kvalifikovaného elektronického razítka nebo na přesnost časového údaje, který je do něj vkládán, společnost eldentity a.s.:

- ihned přeruší vydávání kvalifikovaných elektronických časových razítek, a to do doby, kdy obnoví řádný stav v souladu s postupy stanovenými v plánu pro zvládání krizových situací a v plánu obnovy,
- zveřejní informaci o této události způsobem umožňující dálkový přístup,
- bez prodlení informuje o této události subjekty, se kterými má uzavřeny smluvní vztahy, které mohou být touto událostí dotčeny,
- oznámí informaci o této události dozorovému orgánu.

Pokud má událost vliv na již vydaná kvalifikovaná elektronická časová razítka a v důsledku toho na ně nelze spoléhat, eldentity a.s. zveřejní bezodkladně informaci o této události rovněž nejméně v jednom celostátně distribuovaném deníku (v Hospodářských novinách, Mladé Frontě Dnes či v jiném, v době zveřejnění celostátně distribuovaném deníku) spolu s údaji, na jejichž základě je možné určit, která kvalifikovaná elektronická časová razítka byla touto událostí dotčena.

V případě kompromitace privátního klíče TSU dojde k jeho okamžitému zneplatnění a umístění na seznam zneplatněných certifikátů vydavatele (RCA).

O skutečnosti je informována veřejnost také tak, že je situace popsána na stránkách eldentity a.s., které jsou nepřetržitě dostupné.

6.4.8.5 Kompromitace soukromého klíče nadřízené certifikační autority

V případě kompromitace privátního klíče vydavatele certifikátu pro TSU dojde k jeho okamžitému zneplatnění a umístění na seznam zneplatněných certifikátů vydavatele (RCA). Další postup je popsán v odpovídající Certifikační politice a Certifikační prováděcí směrnici kořenové certifikační autority.

O skutečnosti je informována veřejnost také tak, že je situace popsána na stránkách elidentity a.s., které jsou nepřetržitě dostupné. Je informován neprodleně i dozorový orgán.

6.4.8.6 Schopnost obnovit činnost po havárii

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s plánem pro zvládání krizových situací a plánem obnovy.

6.4.9 Ukončení činnosti TSA

Provozovatel informuje ministerstvo nejméně 3 měsíce před předpokládaným ukončením činnosti. Vynaloží veškeré možné úsilí k tomu, aby vedená evidence byla převzata jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Provozovatel dále informuje doporučeným dopisem každého Žadatele o svém záměru ukončit činnost nejméně 2 měsíce předem.

Provozovatel nejméně 30 dní před ukončením činnosti informuje ministerstvo v případě, že se nepodařilo zajistit převzetí evidence jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti.

6.4.10 Shoda s právními předpisy

Provoz TSA je zabezpečen zcela v souladu s právními předpisy.

6.4.11 Záznam informací o provozu TSA

Auditní záznamy obsahují informace o důležitých událostech provozu systému a obsahují i vydaná časová razítka.

6.4.11.1 Typy zaznamenávaných informací

Archivace dat TSA elidentity je pravidelně provedena jednou měsíčně. Na záznamové médium jsou vypáleny soubory obsahující všechna časová razítka a auditní logy za dané období a za každou TSU. Otisky souborů a čas jejich archivace jsou uvedeny v příloženém souboru, který je elektronicky podepsán.

6.4.11.2 Periodicita zpracování záznamů

Záznamy se archivují jednou měsíčně.

6.4.11.3 Doba uchování auditních záznamů

Pro archivaci jsou vybírána media, u kterých výrobce zaručuje minimální dobu čitelnosti 3 roky. Po dvou letech jsou média přepalována. Celková doba archivace dat je nejméně 10 let.

6.4.11.4 Ochrana auditních záznamů

Práva k prohlížení archivu závisí na sledovaných položkách. Časová razítka může prohlížet každá osoba, která má oprávněný přístup k archivním informacím. Auditní archivní informace jsou přístupné pouze oprávněným osobám prostřednictvím prohlížečů aplikace. Osoby, které mají oprávnění k přístupu, jsou poučeny, že v archivu se mohou vyskytovat osobní údaje.

6.4.11.5 Postupy pro zálohování auditních záznamů

Odpovídají kapitole 6.4.11.1 tohoto dokumentu.

6.4.11.6 Systém shromažďování auditních záznamů (interní nebo externí)

Archivní kopie se ukládají do trezoru.

6.4.11.7 Postup při oznamování události subjektu, který ji způsobil

Neposkytuje se.

6.4.11.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti jsou eskalovány automaticky emailem odpovědné osobě.

6.4.12 Uchovávání informací a dokumentace

6.4.12.1 Typy informací a dokumentace, které se uchovávají

Základními typy informací a dokumentace, které se uchovávají, jsou:

- smlouva o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby,
- vydané kvalifikované elektronické časové razítko,

- prohlášení držitele certifikátu o tom, že mu byly poskytnuty informace o přesných podmínkách pro využívání kvalifikovaných služeb vytvářejících důvěru, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je, či není kvalifikovaným poskytovatelem služeb vytvářejících důvěru.

Společnost eldentity a.s. zajišťuje uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením za podmínek upřesněných v dokumentu ACAeID 22 Plán pro zvládání krizových situací a plán obnovy.

Zaměstnanci eldentity a.s., případně jiné fyzické osoby, které přicházejí do styku s osobními údaji a daty pro vytváření elektronických podpisů, podepisujících osob a elektronických pečetí pečetících osob, zachovávají mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost jejich mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací; uvedené osoby může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

Nakládání s jinými řízenými dokumenty (provozní dokumentace, směrnice, politiky a další interní dokumentace týkající se vývoje a provozování informačních systémů společnosti eldentity a.s.) je prováděno v souladu s pravidly určenými v systému řízení jakosti dle ISO 9001:2008 nebo novější.

6.4.12.2 Doba uchování uchovávaných informací a dokumentace

Veškeré informace a dokumentaci o poskytovaných službách podle Zákon uchovává eldentity po dobu nejméně 10 let.

Doba uchování dalších informací je určena v systému řízení jakosti dle ISO 9001:2008 nebo novější.

6.4.12.3 Zveřejnění certifikátů a CRL

TSA nezveřejňuje certifikáty ani CRL.

6.4.12.4 Zveřejňování informací o autoritě časového razítka

Společnost eldentity a.s. zveřejňuje informace týkající se TSA na svých webových stránkách. Navíc v souladu s bezpečnostní dokumentací zveřejňuje certifikáty svých certifikačních autorit a TSU i jinými nezávislými zdroji na stránkách ministerstva a ve Věstníku ministerstva.

6.4.12.5 Periodicita zveřejňování informací

Informace se zveřejňují průběžně.

6.4.12.6 Řízení přístupu k jednotlivým typům úložišť

Systém je popsán v interní dokumentaci.

6.5 Ostatní obchodní a právní záležitosti

6.5.1 Poplatky

Výše poplatků je uvedena v Ceníku služeb.

6.5.1.1 Poplatky za vydání kvalifikovaných elektronických časových razítek

Výše poplatků za vydání kvalifikovaného elektronického časového razítka je uvedena v Ceníku služeb.

6.5.1.2 Poplatky za přístup k certifikátu poskytovatele

Tato služba je bez poplatků.

6.5.1.3 Poplatky za informace o stavu certifikátu nebo o zneplatnění certifikátu poskytovatele

Tato služba je bez poplatků.

6.5.1.4 Poplatky za další služby

Dle Ceníku služeb.

6.5.2 Finanční odpovědnost

6.5.2.1 Krytí pojištěním

Společnost eIdentity a.s. má uzavřenu pojistku podnikatelských rizik v dostatečné výši, aby byly pokryty případné finanční škody.

6.5.2.2 Další aktiva a záruky

Společnost eIdentity a.s. má připraveny i další kapitálové zdroje, které zajistí poskytování kvalitních certifikačních služeb na požadované úrovni kvality.

6.5.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba se neposkytuje.

6.5.3 Důvěrnost obchodních informací

6.5.3.1 Výčet důvěrných informací

Za neveřejné obchodní informace se považují zejména informace o odebíraných službách, jejich ceny a obchodní smlouvy s nimi svázané. Za další takové informace se považují i smlouvy s třetími stranami, které se podílejí na provozu či jeho zajištění ACAeID, žádosti o poskytnutí služby, auditní a transakční záznamy, havarijní plány a plány obnovy, certifikační prováděcí směrnice, způsoby ochrany osobních údajů, zabezpečení obsluhy systému ACAeID, bezpečnostní opatření a jejich realizace.

Je určeno v systému řízení jakosti dle ISO 9001:2008 nebo novější.

6.5.3.2 Informace mimo rámec důvěrných informací

Za takové jsou považovány informace, které jsou zveřejněné pomocí webových služeb.

6.5.3.3 Odpovědnost za ochranu důvěrných informací

Každý pracovník, který přijde s informacemi dle kapitoly 6.5.3.1 do styku, je nesmí poskytnout třetí straně bez souhlasu odpovědného pracovníka elidentity a.s.

6.5.4 Ochrana osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb.

6.5.5 Práva duševního vlastnictví

Společnost elidentity a.s. zachovává veškerá práva na intelektuální vlastnictví týkající se obsahu certifikátu a revokačních dat, obsahu politik, podle kterých se řídí poskytování služeb vytvářejících důvěru a obsahu jmen, která mohou obsahovat ochranné známky, obchodní či jiné chráněné informace.

6.5.6 Zastupování a záruky

6.5.6.1 Zastupování a záruky TSA

Společnost elidentity a.s. zaručuje, že:

- veškeré údaje v časovém razítku jsou v souladu s interní dokumentací,
- jsou uvedeny pouze správné a pravdivé údaje,
- časová razítka jsou vydána plně v souladu s tímto dokumentem.

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby.

6.5.6.2 Zastupování a záruky třetí strany

V obchodní oblasti může být společnost eldentity a.s. zastupována třetí stranou. V takovém případě je mezi tímto zástupcem a společností eldentity a.s. uzavřena smlouva.

6.5.6.3 Zastupování a záruky zákazníka, odpovědné osoby nebo žadatele

Žadatel, zákazník nebo jím pověřená osoba musí plnit jim uložené povinnosti dle tohoto dokumentu.

6.5.6.4 Zastupování a záruky ostatních zúčastněných subjektů

Spoléhající se strana se zaručuje, že kvalifikované elektronické časové razítko bude používat v souladu s tímto dokumentem.

6.5.7 Zřeknutí se záruk

Společnost eldentity a.s. neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování služeb vytvářejících důvěru, zejména za provozování v rozporu s podmínkami uvedenými v tomto dokumentu, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení apod.

6.5.8 Omezení odpovědnosti

Společnost eldentity a.s. neodpovídá za škodu vyplývající z použití kvalifikovaného elektronického časového razítka, pokud došlo ze strany zákazníka, žadatele anebo spoléhající se strany k nedodržení omezení pro jeho použití, uvedených v této politice a zveřejněných na webových stránkách eldentity a.s.

6.5.8.1 Odpovědnost zákazníka

Zákazník je povinen zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování služeb vytvářejících důvěru,
- neprodleně uvědomit poskytovatele služby vydávání časových razítek o změnách údajů, které jsou ve smlouvě uvedeny, zejména o změnách údajů o pověřených osobách.

6.5.8.2 Odpovědnost pověřených osob

Pověřená osoba je povinna zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o kvalifikované elektronické časové razítko podle této politiky,
- zajistit důvěrnost autentizačních informací, se kterými při registraci žadatelů přichází do styku.

6.5.8.3 Odpovědnost žadatele

Žadatel je povinen zejména:

- zajistit důvěrnost autentizačních informací potřebných pro ověření identity žadatele při podávání žádosti o kvalifikované elektronické časové razítko,
- seznámit se s politikou, podle které mu bylo kvalifikované elektronické časové razítko vydáno.

6.5.8.4 Odpovědnost poskytovatele

Poskytovatel služby vydávání kvalifikovaných elektronických časových razítek je zejména povinen:

- během procesu uzavírání smlouvy o poskytování služeb vytvářejících důvěru ověřit všechny údaje podle předložených dokladů,
- ověřit autentizační údaje žadatele při podání žádosti o vydání časového razítka,
- vydat kvalifikované elektronické časové razítko obsahující věcně správné údaje na základě informací, které jsou TSA k dispozici v době vydávání časového razítka,
- zveřejňovat politiky, podle kterých vydává časová razítka, na webových stránkách eidentity a.s.,
- zveřejnit certifikát TSU tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním Služeb vytvářejících důvěru; náležitá péče zahrnuje zejména provoz v souladu:
 - s platnými právními předpisy,
 - s tímto dokumentem,
 - s provozní dokumentací.

6.5.9 Odpovědnost za škodu, náhrada škody

Odpovědnost za škodu je specifikována ve smlouvě o poskytování služby.

6.5.10 Doba platnosti, ukončení platnosti

6.5.10.1 Doba platnosti

Doba platnosti tohoto dokumentu je od vydání do jeho odvolání. Úpravy dokumentu včetně zajištění souladu politik schvaluje Výbor pro politiky.

6.5.10.2 Ukončení platnosti

Ukončení platnosti tohoto dokumentu je dáno jeho odvoláním. Úpravy dokumentu včetně zajištění souladu politik schvaluje Výbor pro politiky.

6.5.10.3 Důsledky ukončení platnosti

Důsledky jsou v souladu s tímto dokumentem.

6.5.11 Komunikace mezi zúčastněnými subjekty

Veřejné informace, týkající se provozu služby kvalifikovaných elektronických časových razítek, jsou k dispozici na stránkách elidentity a.s. a to i dálkovým přístupem. Smluvní vztahy jsou uzavírány písemně a to v listinné nebo i v elektronické formě.

6.5.11.1 Komunikace s poskytovatelem služby vydávání kvalifikovaných elektronických časových razítek

Žádost o kvalifikované elektronické časové razítko a odpověď na tuto žádost se přepravuje zabezpečeným komunikačním kanálem.

6.5.11.2 Komunikace v rámci ACAeID

Tato komunikace je určena v interní dokumentaci.

6.5.11.3 Komunikační jazyk

Komunikačním jazykem je čeština, pokud se strany nedohodnou jinak.

6.5.12 Změny v CP

6.5.12.1 Postup při změnách

Návrh na úpravu Certifikační politiky podává člen Výboru pro politiky na zasedání Výboru pro politiky. Výbor pracuje v souladu s jednacím řádem a v případě přijetí změny určí osobu zodpovědnou za zapracování změny do Certifikační politiky. Nová CP je na zasedání Výboru pro politiky projednána a vyhlášena.

6.5.12.2 Postup při oznamování změn

Postup probíhá řízeným procesem v souladu s jednacím řádem Výboru pro politiky. Nová Certifikační politika je účinná dnem vyhlášení dle rozhodnutí Výboru pro politiky.

6.5.12.3 Okolnosti, při kterých musí být změněno OID

Změna OID Certifikační politiky je provedena při takových změnách dokumentu, které vedou k povýšení verze dokumentu.

Změna OID se neprovádí při takových změnách dokumentu, které nevedou ke změně verze dokumentu (např. oprava jazykových chyb, překlepů, formátování, vizuálních stylů apod. bez změny smyslu sdělení).

6.5.13 Řešení sporů

Systém je provozován ve shodě s požadavky zákona 297/2016 Sb., 101/2000 Sb. a dalšími požadavky a je provozován jako kvalifikovaný k poskytování kvalifikovaných služeb vytvářejících důvěru.

Všechny vztahy mezi eidentity a.s. a subjekty využívajícími služeb TSA se řídí platnými zákony České Republiky a předpisy souvisejícími.

Pro případ vzniku neshody nebo sporu je postup následující:

- Poškozená strana vypracuje a doručí protistraně písemné oznámení o vzniku a existenci události, která je v neshodě se zákonem, platnou politikou TSA nebo smlouvou, včetně přesného popisu události a vyčíslení případných škod událostí přímo způsobených.
- Protistrana oznámení akceptuje, zajistí nápravu a přijme závazek k úhradě vzniklých škod nebo
- protistrana oznámení neakceptuje a bez zbytečného prodlení vyvolá smírčí jednání za přítomnosti kompetentních zástupců obou stran.
- Strany při smírčím jednání dospějí k dohodě a postupují dále v souladu s výsledky jednání. O průběhu a výsledku smírčího jednání musí být vždy vyhotoven písemný zápis podepsaný oběma stranami nebo
- strany nedospějí k dohodě a poškozená strana dále postupuje právní cestou dle vlastního uvážení.

6.5.14 Rozhodné právo

Platí právo České republiky.

6.5.15 Shoda s právními předpisy

Systém je provozován v souladu s právními předpisy.

6.5.16 Další ustanovení

6.5.16.1 Vyšší moc

Smlouva o poskytnutí služby může obsahovat ustanovení o působení vyšší moci.

6.5.17 Další opatření

6.5.17.1 Použitá literatura a řídicí dokumenty

Systémy společnosti eIdentity a.s. jsou v souladu s těmito dokumenty:

- CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements,
- ČSN ETSI TS 101 456 – Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty,
- ČSN ETSI TS 102 023 – Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek,
- ČSN ISO/IEC 17799 – Informační technologie – Soubor postupů pro management bezpečnosti informací,
- ČSN BS 7799-2 – Systém managementu bezpečnosti informací – Specifikace s návodem pro použití,
- ČSN ISO/IEC TR 13335 – Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3,
- ČSN EN ISO 19011 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu,
- CWA 14167-2 – Cryptographic module for CSP signing operations with backup - Protection profile – CMCSOB PP,
- CWA 14167-4 – Cryptographic module for CSP signing operations – Protection profile – CMCSO PP,
- CWA 14169 – Secure signature-creation devices “EAL 4+”,
- FIPS PUB 140-1 - Security Requirements for Cryptographic Modules,
- FIPS PUB 140-2 - Security Requirements for Cryptographic Modules.
 - ETSI EN 319 401,
 - ETSI EN 319 411,
 - ETSI EN 319 421,
 - ETSI EN 319 422.

6.5.17.2 Návazné dokumenty

Činnost systémů společnosti eIdentity a.s. je určena sadou interní dokumentace. Dokumentace je řízena v souladu s normou ISO9001 nebo novější.

7 ZÁVĚREČNÁ USTANOVENÍ

Tento dokument byl projednán na jednání Výboru pro politiky a podle zápisu byl přijat a vyhlášen.