Česká republika – Ministerstvo životního prostředí

• • •

eIdentity a.s.

SMLOUVA O POSKYTOVÁNÍ ČASOVÝCH RAZÍTEK

Smlouva o poskytování časových razítek (dále jen „**Smlouva**“) je uzavřena níže uvedeného dne, měsíce a roku ve smyslu ustanovení § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**“), a v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“),

mezi

Objednatelem:	**Česká republika – Ministerstvo životního prostředí**
Se sídlem:	Vršovická 1442/65, 100 10 Praha 10
IČO:	00164801
Jednajícím:	Ing. Jana Vodičková, ředitelka odboru informatiky
Bankovní spojení:	ČNB, Praha 1
Číslo účtu:	7628001/0710
Zástupce pro věcná jednání:	Ing. František Zádrapa, Ing. David Špalt

(dále jen „**Centrální zadavatel**“ nebo také „**Objednatel**“)

a

Poskytovatelem:	**eldentity a.s.**
Se sídlem:	Vinohradská 184/2396, 130 00 Praha 3
IČO:	27112489
DIČ:	CZ27112489 (je plátce DPH)
Jednajícím:	Ing. Ladislav Šedivý, předseda představenstva
Bankovní spojení:	Komerční Banka a.s.
Číslo účtu:	51-691110267/0100
Zástupce pro věcná jednání:	Vojtěch Vajs (tel:+420 222 866 150, email: xxxxxxxxxx)
Zapsaným:	obchodní rejstřík vedený Městským soudem v Praze, sp. zn. B9080

(dále jen „**Poskytovatel**“)

(Centrální zadavatel a Poskytovatel společně dále jen jako „**Smluvní strany**“ nebo jednotlivě „**Smluvní strana**“; za Smluvní stranu jsou v kontextu Smlouvy považovány též jednotlivé subjekty Resortu ŽP / Objednatelé oprávnění požadovat na Poskytovateli plnění na základě Smlouvy za podmínek v ní stanovených)

Preambule

Smlouva je uzavírána mezi Centrálním zadavatelem a Poskytovatelem na základě výsledků zadávacího řízení na Část 1 nadlimitní veřejné zakázky na služby s názvem **„Implementace Enterprise infrastruktury digitální důvěry dle eIDAS – etapa 3“**, systémové číslo na profilu Centrálního zadavatele E-ZAK: P18V00001164; evidenční číslo ve Věstníku veřejných zakázek: Z2018-022046 (dále jen „**Veřejná zakázka**“), zadávané v otevřeném řízení v souladu s ustanovením § 3 písm. b) a § 56 a násl. ZZVZ (dále jen „**Zadávací řízení**“). Nabídka Poskytovatele podaná v rámci Zadávacího řízení na Veřejnou zakázku (dále jen „**Nabídka**“) byla Centrálním zadavatelem, jakožto zadavatelem Veřejné zakázky, vyhodnocena jako ekonomicky nejvýhodnější.

Poskytovatel tímto čestně prohlašuje, že je oprávněným poskytovatelem požadovaných služeb a splňuje veškeré podmínky a požadavky ve Smlouvě stanovené, a že tedy Smlouvu uzavřel po pečlivém zvážení všech možných důsledků, přičemž předmět plnění dle Smlouvy není plněním nemožným.

Článek 1
Základní pojmy

Pro účely této Smlouvy se rozumí:

- **Ministerstvem životního prostředí** (dále jen „**MŽP**“) – Centrální zadavatel a další organizační útvary začleněné v organizační struktuře MŽP, které jsou oprávněny na účet MŽP požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem této Smlouvy za podmínek v ní stanovených;
- **Centrálním zadavatelem** – organizační útvar MŽP, který je oprávněn jménem a na účet MŽP a rovněž jménem a na účet Pověřujících zadavatelů uvedených v Příloze č. 1 Smlouvy v souladu s právními a vnitřními předpisy nebo na základě příslušných smluv o centralizovaném zadávání uzavřít tuto Smlouvu a požadovat na Poskytovateli plnění ve formě služeb, které jsou jejím předmětem za podmínek v ní stanovených;
- **Pověřujícím zadavatelem** – právní subjekt uvedený v Příloze č. 1 Smlouvy, který uzavřel s Centrálním zadavatelem příslušnou smlouvu o centralizovaném zadávání a který je oprávněn na základě Smlouvy svým jménem a na svůj účet požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem Smlouvy za podmínek v ní stanovených;
- **Smlouvou o centralizovaném zadávání** – smlouva, popř. smlouvy uzavřené před zahájením centralizovaného Zadávacího řízení na Veřejnou zakázku mezi Centrálním zadavatelem a jednotlivými Pověřujícími zadavateli, v níž si upravili svá vzájemná práva a povinnosti v souvislosti s centralizovaným zajištěním služeb kvalifikovaných poskytovatelů služeb vytvářejících důvěru;
- **Resortem ŽP** – množina subjektů MŽP a Pověřujících zadavatelů v rozsahu dle Přílohy č. 1 Smlouvy;
- **Resortní organizací** – resortní organizace MŽP spadající do Resortu ŽP, která odpovídá též pojmu Pověřující zadavatel v rozsahu dle Přílohy č. 1 Smlouvy;
- **Objednatelem** – subjekt Resortu ŽP, oprávněný požadovat na Poskytovateli plnění Veřejné zakázky na základě vystavení Realizační objednávky dle této Smlouvy, tj. oprávněný na účet MŽP nebo na svůj účet požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem Smlouvy za podmínek v ní stanovených;

- **Oprávněným žadatelem o vydání kvalifikovaného časového razítka respektive elektronického časového razítka** – fyzická nebo právnická osoba, která se prokazuje (autentizuje) v elektronické komunikaci platným komerčním osobním certifikátem nebo komerčním serverovým certifikátem vydaným Poskytovatelem na žádost subjektu Resortu ŽP nebo uživatelským jménem a heslem;
- **Poskytovatelem** – kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikovaná elektronická časová razítka nebo kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající elektronická časová razítka, který byl vybrán jako nejvhodnější v rámci Zadávacího řízení na Veřejnou zakázku;
- **Realizační objednávka** – první a jediná objednávka Objednatele, na jejímž základě započne Poskytovatel poskytovat plnění Veřejné zakázky dle Smlouvy (vzor Realizační objednávky viz Příloha č. 2 Smlouvy).

Seznam použitých zkratek:

- **CPTSA** – certifikační politika pro vydávání kvalifikovaných el. časových razítek / elektronických časových razítek;
- **ETSI** – European Telecommunications Standards Institute;
- **EU** – Evropská unie;
- **HA** – High Availability (neboli vysoká dostupnost);
- **HW** – Hardware;
- **SLA** – dohoda o úrovni poskytovaných služeb;
- **SW** – Software;
- **TSA** – kvalifikovaná elektronická časová razítka / elektronická časová razítka;
- **ŽP** – Životní prostředí.

Článek 2
Účel a předmět Smlouvy

2.1 Účelem Smlouvy je zajištění realizace Veřejné zakázky, resp. úprava podmínek týkajících se poskytování opakujících se služeb, které jsou předmětem plnění dle Smlouvy, zadávaných po dobu její platnosti, a tedy zajištění vydávání TSA pro potřeby Resortu ŽP plně v souladu s jeho potřebami, záměry, projekty a platnými právními předpisy prostřednictvím Poskytovatele.

2.2 Cílem Smlouvy je centralizované zajišťování služeb vytvářejících důvěru poskytovaných kvalifikovaným poskytovatelem služeb vytvářejících důvěru (dále jen „**certifikační služby**“ nebo jen „**služby**“), a to na základě uzavřené Smlouvy pro Část 1 Veřejné zakázky.

2.3 Na základě této Smlouvy bude komplexně zajištěno vydávání TSA vydaných kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále také „**eIDAS**“), resp. zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, pro potřeby Resortu ŽP a dalších subjektů v souladu s platnými certifikačními politikami kvalifikovaných poskytovatelů služeb vytvářejících důvěru pro oblast TSA. V této souvislosti si Poskytovatel v rámci zabezpečení služeb TSA vyhrazuje právo změnit požadavky týkající

se HW a SW vybavení Resortu ŽP, a to zejména z důvodu změny legislativy či technologie, které mohou tyto požadavky na změny vyvolat. Požadavky na změny oznámí Poskytovatel Objednateli písemně nejpozději 30 pracovních dní před jejich zavedením.

2.4 Předmětem Smlouvy je tedy povinnost Poskytovatele vydávat kvalifikovaná elektronická časová razítka vydaná kvalifikovaným poskytovatelem a související služby, přičemž:

a) požadavky Objednatelů na vydání kvalifikovaného elektronického časového razítka budou vydávány z jednotlivých aplikací provozovaných v Resortu ŽP (např. z centrálního řešení infrastruktury digitální důvěry dle eIDAS Resortu ŽP, spisové služby apod.);

b) kvalifikovaná elektronická časová razítka budou poskytována pomocí webové služby dostupné v režimu 7x24 (kromě předem definovaných plánovaných technických odstávek předem oznámených Oprávněným osobám dle článku 4 Smlouvy), která bude volána z definovaných aplikací;

c) Poskytovatel musí být schopen rozdělit čerpání TSA dle MŽP a jednotlivých Resortních organizací; MŽP a každá Resortní organizace musí mít vlastní přihlašovací údaje (login a heslo nebo certifikát);

d) MŽP a jednotlivé Resortní organizace musí mít přístup na webový portál Poskytovatele pro kontrolu počtu čerpání časových razítek dle jednotlivých organizací Resortu ŽP; každá Resortní organizace bude mít k dispozici informace o vlastním čerpání časových razítek, MŽP bude mít k dispozici všechny informace za Resort ŽP;

e) Poskytovatel musí předložit popis doporučeného technického řešení a popis jeho integrace do systémů, které budou vyžadovat pořízení kvalifikovaného časového razítka:

- činnosti a opatření, která musí být realizována na straně integrované aplikace Resortu ŽP;
- činnosti a opatření na straně Poskytovatele (povolení volání WS apod.) a popis komunikace mezi Resortem ŽP a Poskytovatelem při integraci nové aplikace.

2.5 Plnění musí vyhovovat bezpečnostním standardům, jejichž použití je obvyklé u obdobných produktů, a musí svou technickou úrovní odpovídat podmínkám Resortu ŽP v oblasti bezpečnosti a provozu informačních a komunikačních technologií.

2.6 Dále je předmětem Smlouvy závazek Smluvních stran zachovávat mlčenlivost o všech údajích o Smluvních stranách či třetích osobách, majících charakter utajovaných informací dle ustanovení zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „**zákon o ochraně utajovaných informací**“), a charakter osobních údajů dle ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**zákon o ochraně osobních údajů**“), a Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „**nařízení GDPR**“). Smluvní strany jsou si vzájemně rovněž povinny na žádost druhé Smluvní strany prokázat způsob, jakým je dodržování povinností stanovených příslušným zákonem zajištěno.

2.7 Předmětem Smlouvy je rovněž závazek Objednatelů platit Poskytovateli za řádné poskytování služeb dle této Smlouvy cenu dle článku 6 a 7 této Smlouvy.

Článek 3
Realizační objednávka

3.1 Na veškeré služby, které budou poskytovány na základě Smlouvy, se budou vztahovat práva a povinnosti Smluvních stran vymezené ve Smlouvě. Realizační objednávky budou uzavírány v souladu s podmínkami Smlouvy.

3.2 Realizační objednávka Objednatele k poskytnutí plnění dle Smlouvy, jejíž vzor je dán Přílohou č. 2 této Smlouvy (dále jen „**Objednávka**"), musí obsahovat alespoň níže uvedené údaje:

a) číslo Objednávky;

b) identifikační a fakturační údaje Objednatele;

c) vymezení a popis požadovaného plnění (předpokládaný počet TSA);

d) dobu a místo plnění;

e) další požadavky Objednatele na předmět plnění v souladu se Smlouvou;

f) podpis oprávněné osoby Objednatele (viz článek 5 Smlouvy).

Článek 4
Místo a doba plnění a způsob poskytování předmětu plnění

4.1 Místy plnění služeb a oprávněnými Objednateli jsou všechna místa uvedená v Příloze č. 1 Smlouvy.

4.2 Předmět plnění dle Smlouvy bude Poskytovatelem zajišťován průběžně, a to na základě Objednávek, které budou za Objednatele realizovat jimi pověřené oprávněné osoby dle článku 5 Smlouvy.

4.3 Objednávka bude jednotlivými Objednateli a jejich oprávněnými osobami dle článku 5 Smlouvy vystavena pouze při prvním objednání služeb a bude obsahovat veškeré náležitosti uvedené v článku 3 odst. 3.2 Smlouvy.

4.4 Objednávky budou zasílány Objednatelem písemnou formou na kontaktní email Poskytovatele info@eidentity.cz a xxxxxxxxxx, a to nejpozději 48 hodin před termínem prvního plnění. Povinností Poskytovatele je tuto Objednávku obratem písemně Objednateli potvrdit na kontaktní email Objednatele uvedený v Příloze č. 1 Smlouvy a zároveň zaslat přihlašovací údaje (uživatel, heslo) nebo potvrzení o zaregistrování příslušného komerčního certifikátu k odběru služby.

4.5 Smluvní strany berou na vědomí, že práva a povinnosti Smluvních stran Objednávkou neupravené odpovídají právům a povinnostem Objednatele a Poskytovatele stanoveným Smlouvou.

Článek 5
Oprávněné osoby a komunikace Smluvních stran

5.1 Jednotlivé Objednávky předkládané podle Smlouvy jsou jménem subjektů Resortu ŽP uvedených v Příloze č. 1 Smlouvy (Objednatelů) oprávněni podepisovat vedoucí zaměstnanci oprávnění k zastupování příslušného subjektu Resortu ŽP nebo jimi zmocněné osoby (dále jen „**Oprávněná osoba**").

5.2 Objednatel je oprávněn z vlastního podnětu nebo jemu adresovaných podnětů subjektů Resortu ŽP v případě potřeby jednostranně seznam Oprávněných osob měnit včetně jeho rozšíření.

Veškeré změny v seznamu Oprávněných osob musí být dostatečně transparentní a musí být patrno, kterých Oprávněných osob se týkají, případně které Oprávněné osoby mají být ze seznamu vypuštěny nebo do seznamu přidány a k jakému datu. Poskytovatel je povinen v souvislosti s jím poskytovanými službami realizovat takové změny na základě písemné žádosti Objednatele předané na adresu sídla Poskytovatele nebo na emailovou adresu info@eidentity.cz a xxxxxxxxxx nejpozději 2 pracovní dny před datem požadované změny.

Článek 6
Cenové podmínky

6.1 Cena 1 kus (jednotku) TSA vydaného Poskytovatelem Objednateli dle Objednávky (dále jen „**jednotková cena**“) činí 0,09 Kč (slovy: devět haléřů) bez daně z přidané hodnoty (dále jen „**DPH**“). DPH činí v souladu s aktuálně platnou a účinnou právní úpravou 21 %, tedy 0,02 Kč (slovy: dva haléře). Jednotková cena včetně DPH tak činí 0,11 Kč (slovy: jedenáct haléřů). V takto stanovené jednotkové ceně je již zohledněna cena za vydání autorizačních komerčních certifikátů a veškeré náklady spojené s poskytováním příslušných služeb, poštovné, poplatky, administrativní práce, cestovní náklady, jakož i další běžné výdaje spojené s poskytováním sjednaných služeb. Náhrada mimořádných hotových výdajů souvisejících s poskytovanými službami se nepřipouští. Tato jednotková cena je nejvýše přípustná a nepřekročitelná s výjimkou postupu dle článku 7 odst. 7.9 této Smlouvy.

6.2 Cena za plnění Smlouvy bude stanovena jako součin skutečně odebraného počtu TSA v příslušném kalendářním čtvrtletí a jednotkové ceny za 1 kus TSA dle odst. 6.1 tohoto článku (dále také jako „**čtvrtletní cena**“).

6.3 Čtvrtletní cena bude účtována (fakturována) Poskytovatelem jednotlivým Objednatelům v Resortu ŽP podle jimi skutečně odebraného počtu TSA v daném kalendářním čtvrtletí. Skutečně odebraný počet TSA musí odpovídat přehledu odebraných TSA uvedenému na www stránkách Poskytovatele: www.eidentity.cz v souladu s článkem 2 odst. 2.4 písm. c) a d) této Smlouvy. Přehled odebraných TSA bude na výše uvedené www stránce Poskytovatele denně aktualizován a data budou Objednateli dostupná vždy za období posledních 12 měsíců.

Článek 7
Platební podmínky

7.1 Úhrady čtvrtletní ceny dle článku 6 odst. 6.2 Smlouvy budou prováděny samostatně jednotlivými Objednateli, a to vždy zpětně za certifikační služby odebrané v předchozím kalendářním čtvrtletí na základě Poskytovatelem vystaveného řádného daňového a účetního dokladu (dále také „**faktura**“).

7.2 Každá faktura musí být Objednateli vystavena a doručena podle skutečně dodaného objemu certifikačních služeb pro daného Objednatele za uplynulé kalendářní čtvrtletí do 10 kalendářních dnů po datu uskutečnění zdanitelného plnění, kterým je poslední den příslušného kalendářního čtvrtletí.

7.3 Právo fakturovat certifikační služby vzniká po převzetí čtvrtletního přehledu odebraných časových razítek a jeho potvrzení Oprávněnou osobou Objednatele v místě plnění.

7.4 Každá faktura bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Jedná se především o označení každé faktury a její číslo, identifikační údaje Objednatele, specifikaci předmětu plnění podle Smlouvy včetně

čísla Objednávky Objednatele, bankovní spojení, fakturovanou částku bez/včetně DPH, sazba DPH. Faktura bude mít náležitosti obchodní listiny dle § 435 Občanského zákoníku. Každá faktura bude rovněž označena evidenčním číslem Smlouvy z Centrální evidence smluv Centrálního zadavatele: 170217 (viz také záhlaví Smlouvy).

7.5 Nebude-li jakákoli faktura obsahovat náležitosti daňového dokladu dle odst. 7.4 tohoto článku Smlouvy, nebo bude-li obsahovat jiné cenové údaje nebo jiný druh či množství předmětu plnění než dohodnutý ve Smlouvě, či bude-li chybět potvrzený čtvrtletní přehled odebraných TSA dle odst. 7.3 tohoto článku Smlouvy, nepovažuje se faktura za řádný daňový a účetní doklad, neběží doba splatnosti a Objednatel je oprávněn fakturu vrátit s tím, že Poskytovatel je poté povinen vystavit novou fakturu s novým termínem splatnosti, přičemž doba splatnosti běží teprve od okamžiku doručení nové faktury Objednateli. V takovém případě není Objednatel v prodlení s placením faktury.

7.6 Lhůta splatnosti řádně vystavené faktury činí 30 kalendářních dnů ode dne jejího doručení Objednateli. Povinnost Objednatele zaplatit fakturovanou částku je splněna dnem odepsání příslušné částky z účtu Objednatele. Veškeré platby dle Smlouvy budou probíhat výlučně bezhotovostním převodem na účet Poskytovatele uvedený v identifikačních údajích Poskytovatele ve Smlouvě a na každé faktuře.

7.7 Objednatel neposkytuje žádné zálohové platby. Veškeré platby budou probíhat výhradně v Kč (CZK), rovněž veškeré cenové údaje na faktuře budou v této měně.

7.8 Překročení stanovených cen uvedených v článku 6 Smlouvy se nepřipouští.

7.9 Jednotkovou včetně DPH uvedenou v čl. 6 odst. 6.1 této Smlouvy je možné změnit pouze v případě, že dojde v průběhu realizace Smlouvy ke změnám daňových předpisů upravujících výši DPH. DPH bude v takovém případě k jednotkovým cenám bez DPH účtována ve výši v souladu s právní úpravou platnou ke dni uskutečnění zdanitelného plnění.

Článek 8
Práva a povinnosti Poskytovatele

8.1 Poskytovatel prohlašuje, že disponuje všemi příslušnými oprávněními k podnikání a veškerými technickými, ekonomickými i personálními předpoklady nezbytnými pro řádné plnění předmětu Smlouvy. Poskytovatel dále prohlašuje, že je buď kvalifikovaným poskytovatelem služeb vytvářejících důvěru, který vydává kvalifikovaná elektronická časová razítka, případně, že je kvalifikovaný poskytovatel služeb vytvářející důvěru vydávající elektronická časová razítka.

8.2 Poskytovatel je vždy povinen při poskytování sjednaných služeb dle Smlouvy postupovat s odbornou péčí, v souladu se svými povinnostmi stanovenými Smlouvou a v souladu s obecně závaznými právními předpisy.

8.3 Poskytovatel se zavazuje, že předmět plnění bude věcně a právně bezvadný a odpovídající právním předpisům a závazným i doporučujícím normám platným v České republice a členských státech EU.

8.4 Poskytovatel se zavazuje nahradit Objednateli veškerou škodu, která mu vznikne při realizaci Smlouvy v případě, že poskytované plnění se ukáže být nedostatečné, neúplné a/nebo v rozporu se Smlouvou či s právními předpisy.

8.5 Poskytovatel tímto čestně prohlašuje, že mu nejsou známy žádné okolnosti, které by bránily uzavření Smlouvy a plnění závazků z ní vyplývajících.

8.6 Poskytovatel čestně prohlašuje, že má veškerá osvědčení, povolení a/nebo souhlasy či jakákoliv jiná rozhodnutí nezbytná pro řádné plnění jejich povinností vyplývajících ze Smlouvy.

8.7 Poskytovatel tímto prohlašuje, že není předlužen a není mu známo, že by bylo vůči němu zahájeno insolvenční řízení. Dále prohlašuje, že vůči němu není vydáno žádné soudní rozhodnutí, či rozhodnutí správního, daňového či jiného orgánu nebo rozhodce na plnění, které by mohlo být důvodem soudní exekuce na majetek Poskytovatele, nebo by mohlo mít jakkoliv negativní vliv na schopnost Poskytovatele splnit povinnosti vyplývající ze Smlouvy, a že takové řízení nebylo vůči nim zahájeno.

8.8 Poskytovatel zajišťuje plnění formou služby specifikované Smlouvou v souladu se závazným prohlášením dle odst. 8.1 tohoto článku Smlouvy. Poskytovatel se zavazuje poskytovat jednotlivým subjektům Resortu ŽP jako oprávněným žadatelům o služby časové autority danou službu pro jimi realizovaná řešení v souladu s platnou CPTSA Poskytovatele.

8.9 Poskytovatel se zavazuje poskytovat Resortu ŽP podporu zaručenou platnou CPTSA. Aktuální platné znění CPTSA ke dni podpisu Smlouvy je uvedeno v Příloze č. 3 této Smlouvy. Poskytovatel je povinen při každé změně CPTSA o této skutečnosti písemně informovat Objednatele a zaslat mu znění změněné aktuální verze CPTSA. Tato změna nevyžaduje vytvoření dodatku ke Smlouvě.

8.10 Poskytovatel garantuje dostupnost služby časové autority SLA 99,5 % za běžný kalendářní rok v nepřetržitém režimu 24 hodin denně 7 dní v týdnu (365 x 24) po celou dobu platnosti Smlouvy. Do doby 0,5 % možné nedostupnosti nejsou zahrnuty plánované a ohlášené odstávky služby (v délce maximálně 4 hodiny v mimopracovní době 22:00 – 06:00 hod či ve dnech pracovního volna a státem uznaných svátcích), jež je Poskytovatel povinen ohlásit subjektům Resortu ŽP nejméně 7 dní předem. Maximální jednorázová doba nedostupnosti činí maximálně 30 minut. Poskytovatel je dále povinen pravidelně kontrolovat, zda je systém vydávání TSA nakonfigurován v souladu s příslušnými právními předpisy.

8.11 Poskytovatel se zavazuje poskytovat Oprávněným osobám Centrálního zadavatele měsíční statistiky odběru TSA, a to v členění podle jednotlivých Objednatelů a oprávněných žadatelů autentizujících se ke službě odběru TSA z přístupových míst definovaných Objednatelem vždy za uplynulý kalendářní měsíc do 10. dne kalendářního měsíce následujícího. Počet přístupových míst není omezen. Poskytovatel se zavazuje ve shodné lhůtě poskytovat Oprávněným osobám Pověřujících zadavatelů měsíční statistiky odběru TSA, a to v členění podle jednotlivých Oprávněných žadatelů autentizujících se ke službě odběru TSA.

8.12 Poskytovatel se zavazuje poskytovat službu TSA s minimální propustností 10 ks TSA/s.

8.13 Poskytovatel se taktéž zavazuje:

a) zajistit, aby vydaná TSA obsahovala všechny náležitosti stanovené příslušnými obecně závaznými právními předpisy;

b) zajistit, aby časový údaj vložený do TSA odpovídal hodnotě koordinovaného světového času při vytváření časového razítka;

c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání TSA, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném TSA;

d) přijmout odpovídající opatření proti padělání TSA;

e) používat pro účely vydávání časových razítek certifikáty, jejichž rozmezí platnosti musí být stanoveno tak, aby certifikáty byly platné minimálně následující 3 roky od vydání časového razítka.

Článek 9
Práva a povinnosti Objednatele

9.1 Resort ŽP se zavazuje ve svých projektech využívajících TSA, vydaná jako plnění na základě Smlouvy, zabezpečit dodržování platné CPTSA Poskytovatele, jejíž aktuální znění je uvedeno na webu Poskytovatele www.eidentity.cz. Veškeré změny a doplňky tohoto dokumentu dle článku 8 odst. 8.9 Smlouvy jsou vůči Resortu ŽP účinné v souladu s článkem 2 odst. 2.3 Smlouvy. Tyto změny a doplňky však nemají vliv na obsah plnění předmětu a cenu plnění dle Smlouvy.

9.2 Objednatel se zavazuje poskytnout Poskytovateli úplné, pravdivé a včasné informace potřebné k řádnému plnění závazků Poskytovatele.

9.3 Objednatel poskytne Poskytovateli veškerou součinnost, která se v průběhu plnění závazků Poskytovatele dle Smlouvy projeví jako potřebná a zavazuje se zajistit dostatečnou spolupráci ze strany zaměstnanců Objednatele.

9.4 Objednatel bude na základě Smlouvy objednávat certifikační služby, které bude financovat z vlastních zdrojů.

Článek 10
Odpovědnost za vady

10.1 Poskytovatel odpovídá za řádné, odborné a včasné poskytnutí služeb dle Smlouvy.

10.2 Poskytovatel prohlašuje, že předmět plnění dle Smlouvy je bez právních vad, zejména že není a nebude zatížen žádnými právy třetích osob, z nichž by pro Resort ŽP vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany nebo které by jakkoliv omezovalo užití předmětu plnění. V případě porušení tohoto závazku je Poskytovatel v plném rozsahu odpovědný za případné následky takového porušení, přičemž právo Resortu ŽP na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.

10.3 Poskytovatel po dobu účinnosti Smlouvy a závazků z ní plynoucích odpovídá a ručí za to, že předmět plnění bude v souladu se Smlouvou a podmínkami a náležitostmi stanovenými platnými právními předpisy. Poskytovatel zejména odpovídá za shodu funkčního chování a vlastností předmětu plnění s dodanou dokumentací a za garantovanou použitelnost předmětu plnění pro účely vyplývající ze Smlouvy.

10.4 Subjekt Resortu ŽP je oprávněn kdykoliv v průběhu doby platnosti a účinnosti Smlouvy a závazků z ní plynoucích uplatnit vady předmětu plnění u Poskytovatele bez ohledu na to, kdy takové vady zjistil nebo mohl zjistit.

10.5 Poskytovatel nenese odpovědnost za neposkytnutí služby, za zhoršení její kvality nebo za prodlení s jejím poskytnutím, pokud:

a) bude zaviněno jednáním nebo opomenutím subjektu Resortu ŽP, jeho zaměstnanců nebo třetích osob jemu smluvně zavázaných;

b) vznikne v průběhu nutné plánované údržby nebo nutné odstávky systémů Poskytovatele nahlášené subjektu Resortu ŽP nejméně 7 dní před termínem plánované údržby nebo nutné odstávky v souladu s postupy uvedenými ve Smlouvě;

c) bude způsobeno působením vyšší moci, resp. okolnostmi vylučujícími odpovědnost;

d) bude způsobeno ukončením poskytování služeb dle článku 13 Smlouvy.

Článek 11
Odpovědnost za škodu, smluvní pokuty a úrok z prodlení

11.1 Smluvní strany nesou odpovědnost za způsobenou škodu v rámci platných právních předpisů a Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

11.2 Žádná ze Smluvních stran není odpovědna za škodu způsobenou prodlením druhé Smluvní strany s jejím vlastním plněním.

11.3 Žádná ze Smluvních stran není odpovědná za prodlení způsobené okolnostmi vylučujícími odpovědnost dle § 2913 a násl. Občanského zákoníku. Za okolnost vylučující odpovědnost se považuje mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na vůli příslušné Smluvní strany. Překážka vzniklá z osobních poměrů Smluvní strany nebo vzniklá až v době, kdy byla příslušná Smluvní strana s plněním smluvené povinnosti v prodlení, ani překážka, kterou byla příslušná Smluvní strana povinna překonat, povinnosti k náhradě škody nezprostí.

11.4 Smluvní strany se zavazují upozornit druhou Smluvní stranu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění Smlouvy, jejich důsledky, povahu či zánik. Zpráva musí být podána písemně, neprodleně poté, kdy se povinná Smluvní strana o překážce dozvěděla, nebo při náležité péči mohla dozvědět. Bezprostředně po zániku takové překážky povinná Smluvní strana obnoví plnění svých závazků vůči druhé Smluvní straně a učiní vše, co je v jejích silách, pro kompenzaci doby, která uplynula v důsledku takového prodlení. Pokud překážka nepomine do 3 pracovních dnů od doby jejího vzniku, oprávnění zástupci obou Smluvních stran se sejdou za účelem projednání dalšího postupu při plnění závazků vyplývajících ze Smlouvy.

11.5 Poskytovatel neodpovídá za škodu, pokud:

a) bude zaviněno jednáním nebo opomenutím subjektu Resortu ŽP, jeho zaměstnanců nebo třetích osob jemu smluvně zavázaných, včetně nesprávného nebo neoprávněného využívání certifikačních služeb na straně Resortu ŽP;

b) vznikne v průběhu nutné plánované údržby nebo nutné odstávky systémů Poskytovatele nahlášené subjektu Resortu ŽP nejméně 7 dní před termínem plánované údržby nebo nutné odstávky v souladu s postupy uvedenými ve Smlouvě;

c) bude způsobeno působením vyšší moci, resp. okolnostmi vylučujícími odpovědnost;

d) bude způsobeno ukončením poskytování služeb dle článku 13 Smlouvy.

11.6 Poskytovatel odpovídá Centrálnímu zadavateli a jednotlivým Objednatelům za škodu způsobenou při plnění závazků ze Smlouvy v důsledku porušení povinností vyplývajících z obecně závazných právních předpisů či z této Smlouvy.

11.7 Smluvní strany se zavazují, že vždy před uplatněním nároku na náhradu škody písemně vyzvou povinnou Smluvní stranu k jednání o způsobu stanovení výše škody, a to bez zbytečného odkladu poté, kdy se oprávněná Smluvní strana prokazatelně dozví o vzniku škodní události.

11.8 Škody, které Smluvní straně prokazatelně vzniknou v souvislosti s činností druhé Smluvní strany, se povinná Smluvní strana zavazuje zaplatit oprávněné Smluvní straně v plné výši vedle smluvní pokuty na základě samostatné faktury vystavené oprávněnou Smluvní stranou dle Smlouvy.

11.9 V případě překročení nedostupnosti 0,5 % uvedené v článku 8 odst. 8.10 Smlouvy o více než 1 hodinu za kalendářní rok je Poskytovatel povinen uhradit Objednateli smluvní pokutu za 1. takovou hodinu 10.000,- Kč (slovy: deset tisíc korun českých) a za každou další započatou hodinu 20.000,- Kč (slovy: dvacet tisíc korun českých).

11.10 V případě nesplnění minimální propustnosti 10 ks TSA/s uvedené v článku 8 odst. 8.12 Smlouvy je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za takové porušení. Za každé další porušení tohoto ustanovení je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 20.000,- Kč (slovy: dvacet tisíc korun českých).

11.11 V případě prodlení Poskytovatele s plněním povinností uvedených v článku 7 odst. 7.2 a článku 8 odst. 8.11 Smlouvy v termínu dle Smlouvy či příslušných právních předpisů má příslušný subjekt Resortu ŽP/Objednatel právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 0,5 % z celkové ceny včetně DPH za příslušný kalendářní měsíc, a to za každý i započatý den prodlení.

11.12 V případě, že některá ze Smluvních stran poruší některou z povinností uložených článkem 15 Smlouvy, má druhá Smluvní strana právo účtovat jí smluvní pokutu ve výši 20.000,- Kč (slovy: dvacet tisíc korun českých) za každý případ takového porušení.

11.13 Poskytovatel je povinen zaplatit oprávněné Smluvní straně za prodlení s úhradou smluvní pokuty po sjednané lhůtě splatnosti úrok z prodlení ve výši 1 % z dlužné částky pokuty za každý, byť i započatý, den prodlení. Výše sankce není omezena.

11.14 Subjekt Resortu ŽP je povinen zaplatit Poskytovateli za prodlení s úhradou faktury po sjednané lhůtě splatnosti úrok z prodlení ve výši dle příslušných aktuálních právních předpisů za každý, byť i započatý, den prodlení. Výše sankce není omezena.

11.15 Smluvní pokuty a úrok z prodlení jsou splatné do 30 kalendářních dnů od doručení výzvy k úhradě povinné Smluvní straně.

11.16 Zaplacením smluvní pokuty či úroku z prodlení není dotčen nárok Smluvních stran na náhradu škody v plném rozsahu, ani právo odstoupit od Smlouvy. Povinnost Poskytovatele dále řádně poskytovat plnění podle Smlouvy trvá, pokud nedojde k jejímu ukončení dle čl. 13 Smlouvy. Odstoupením od Smlouvy nezaniká nárok na smluvní pokutu či vzniklou škodu.

Článek 12
Pojištění odpovědnosti za škodu

12.1 Poskytovatel prohlašuje, že má ke dni uzavření Smlouvy uzavřenu pojistnou smlouvu pro případ odpovědnosti za škodu způsobenou třetí osobě při poskytování služeb s minimálním limitem pojistného plnění ve výši 5.000.000,- Kč (slovy: pět milionů korun českých) na jednu pojistnou událost (dále jen „**Pojištění odpovědnosti za škodu**“).

12.2 Poskytovatel se zavazuje po celou dobu trvání Smlouvy udržovat sjednané Pojištění odpovědnosti za škodu v minimální výši, jak je uvedeno shora.

12.3 Poskytovatel není oprávněn snížit výši pojistného krytí nebo podstatným způsobem změnit podmínky Pojištění odpovědnosti za škodu bez předchozího písemného souhlasu Centrálního zadavatele.

12.4 Poskytovatel je povinen kdykoliv po dobu trvání Smlouvy Centrálnímu zadavateli na základě jeho výzvy předložit bez zbytečného odkladu doklad o platnosti příslušného Pojištění odpovědnosti za škodu.

12.5 Poskytovatel je povinen neprodleně informovat Centrálního zadavatele o všech změnách v podmínkách Pojištění odpovědnosti za škodu, zejména o výši limitu pojistného plnění a příslušných výlukách z Pojištění odpovědnosti za škodu.

Článek 13
Platnost a účinnost Smlouvy

13.1 Smlouva se uzavírá na dobu určitou, a to maximálně v délce 5 let (60 měsíců) ode dne nabytí její účinnosti dle článku 18 odst. 18.8 Smlouvy, nebo do vyčerpání maximální hodnoty (limitu) Smlouvy ve výši 2.000.000,- Kč bez DPH, a to podle toho, která skutečnost nastane dříve.

13.2 Smlouva může být ukončena jedním z níže uvedených způsobů:

a) písemnou dohodou Smluvních stran;

b) odstoupením od Smlouvy;

c) výpovědí ze strany Objednatele, a to i bez udání důvodů, s výpovědní dobou v délce 3 kalendářních měsíců; výpovědní doba počne běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi Poskytovateli;

d) výpovědí ze strany Poskytovatele, a to i bez udání důvodů, s výpovědní dobou v délce 6 kalendářních měsíců; výpovědní doba počne běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi Objednateli.

Jakýkoli úkon vedoucí k ukončení Smlouvy musí být učiněn v písemné formě a je účinný okamžikem jeho doručení druhé Smluvní straně, není-li ve Smlouvě stanoveno jinak.

13.3 Objednatel je oprávněn odstoupit od Smlouvy, zejména v případě podstatného porušení smluvních povinností dle článku 12 odst. 12.1 a násl. Smlouvy.

13.4 Objednatel je rovněž oprávněn odstoupit od Smlouvy, jestliže zjistí, že:

a) Poskytovatel nabízel, dával, přijímal nebo zprostředkovával nějaké hodnoty s cílem ovlivnit chování nebo jednání kohokoliv, ať již státního úředníka nebo někoho jiného, přímo nebo nepřímo, v Zadávacím řízení nebo při provádění Smlouvy; nebo

b) Poskytovatel zkresloval skutečnosti za účelem ovlivnění Zadávacího řízení nebo provádění Smlouvy ke škodě Objednatele, včetně podvodných praktik k potlačení a snížení výhod volné a otevřené soutěže;

c) vůči majetku Poskytovatele probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku či byl insolvenční návrh zamítnut proto, že majetek Poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení;

d) Poskytovatel vstoupí do likvidace;

e) Poskytovatel bude odsouzen za úmyslný trestný čin;

f) Poskytovateli byla odebrána oprávnění, která jsou pro výkon jeho činnosti v návaznosti na poskytování předmětu Smlouvy vyžadována platnými právními předpisy.

13.5 Smluvní strany jsou oprávněny odstoupit od Smlouvy z důvodů uvedených ve Smlouvě, a dále v případě podstatného porušení Smlouvy ve smyslu ustanovení § 2002 Občanského zákoníku, pokud podstatné porušení Smlouvy, které je důvodem pro odstoupení, nebylo způsobeno okolnostmi vylučujícími odpovědnost dle ustanovení § 2913 odst. 2 Občanského zákoníku.

13.6 Smluvní strany jsou oprávněny odstoupit od Smlouvy z důvodů uvedených v zákoně a dále z důvodů uvedených ve Smlouvě, zejména v případě podstatného porušení Smlouvy ve smyslu ustanovení § 2002 Občanského zákoníku, pokud podstatné porušení Smlouvy, které je důvodem pro odstoupení, nebylo způsobeno okolnostmi vylučujícími odpovědnost dle ustanovení § 2913 odst. 2 Občanského zákoníku.

13.7 Za podstatné porušení Smlouvy Poskytovatelem, které je důvodem pro odstoupení Objednatele od Smlouvy, se považuje:

a) přerušení poskytování služby TSA na více než 3 kalendářní dny;

b) realizace předmětu Smlouvy v rozporu s právními předpisy nebo Smlouvou;

c) jiné porušení povinností Poskytovatele, které nebude odstraněno do 10 kalendářních dní od doručení výzvy Objednatele Poskytovateli.

13.8 Za podstatné porušení Smlouvy ze strany Resortu ŽP, které je důvodem pro odstoupení od Smlouvy Poskytovatelem, se považuje:

a) prodlení Objednatele s úhradou faktury o více než 30 kalendářních dní, přičemž nárok na úrok z prodlení není tímto ustanovením dotčen;

b) prodlení s poskytnutím součinnosti o více než 30 kalendářních dní od prokazatelného doručení písemné výzvy ze strany Poskytovatele.

13.9 Pro podstatné porušení Smlouvy může oprávněná Smluvní strana odstoupit od Smlouvy bez zbytečného odkladu. Odstoupení musí mít písemnou formu, musí v něm být uveden odkaz na ujednání Smlouvy či ustanovení právních předpisů, které zakládá oprávnění od Smlouvy odstoupit, musí být podepsáno oprávněným zástupcem Smluvní strany, která činí právní jednání, a doručeno druhé Smluvní straně. Účinky odstoupení nastanou dnem následujícím po doručení projevu vůle od Smlouvy odstoupit druhé Smluvní straně.

13.10 Objednatel má v případě odstoupení od Smlouvy nárok na náhradu škody spočívající v náhradě prokazatelných nákladů, které mu vzniknou v souvislosti se zajištěním náhradního plnění.

13.11 Odstoupení od Smlouvy se nedotýká nároku na náhradu škody, smluvních pokut, ochrany neveřejných informací, zajištění pohledávky kterékoliv ze Smluvních stran, řešení sporů a ustanovení týkajících se těch práv a povinností, z jejichž povahy toto vyplývá.

Článek 14
Mlčenlivost, ochrana informací a osobních údajů

14.1 Smluvní strany se zavazují udržovat v tajnosti a nezpřístupnit třetím osobám důvěrné informace (jak jsou vymezeny níže). Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.

14.2 Smluvní strany budou považovat ve smyslu Smlouvy za důvěrné:

a) informace poskytnuté ze strany Resortu ŽP Poskytovateli v souvislosti s přípravou a realizací Smlouvy výslovně označené jako důvěrné;

b) informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti;

c) veškeré další informace, které byly Centrálním zadavatelem v zadávacích podmínkách označeny jako důvěrné ve smyslu ustanovení § 218 odst. 1 ZZVZ;

d) utajované informace ve smyslu zákona o ochraně utajovaných informací a osobní údaje ve smyslu zákona o ochraně osobních údajů a nařízení GDPR, informace u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o Resortu ŽP, které by mohly z povahy věci být považovány za důvěrné, a které se Smluvní strany dozvědí v souvislosti s plněním Smlouvy.

14.3 Smluvní strany se zavazují, že nezpřístupní jakékoliv třetí osobě důvěrné informace druhé Smluvní strany bez jejího souhlasu, a to v jakékoliv formě, a že podniknou všechny nezbytné kroky k zabezpečení těchto informací. Poskytovatel je povinen zabezpečit veškeré důvěrné informace Resortu ŽP proti odcizení nebo jinému zneužití. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti po dobu 6 let po ukončení platnosti Smlouvy, není-li zvláštním právním předpisem pro určitou skupinu informací stanovena lhůta delší.

14.4 Smluvní strany se zavazují chránit důvěrné informace druhé Smluvní strany v režimu obvyklé ochrany obchodního tajemství, není-li zvláštním právním předpisem stanoveno jinak.

14.5 Žádná ze Smluvních stran není oprávněna důvěrné informace podle Smlouvy, týkající se druhé Smluvní strany, se kterými byla při své činnosti seznámena nebo které při poskytování služeb získala, využívat v rozporu s oprávněnými zájmy druhé Smluvní strany.

14.6 Smluvní strany jsou povinny vytvářet podmínky pro zabezpečení ochrany informací důvěrného charakteru a jejich ochranu zajistit.

14.7 Smluvní strany jsou oprávněny využívat důvěrné informace pouze a výhradně pro účely spolupráce vyplývající ze Smlouvy.

14.8 Smluvní strany jsou povinny zabezpečit, že povinnosti vyplývající ze Smlouvy budou dodržovány všemi zaměstnanci, pokud tito zaměstnanci získají nebo jsou jim k dispozici informace důvěrného charakteru.

14.9 Na základě výše uvedeného se Smluvní strany zavazují:

a) neposkytnout důvěrné informace získané v písemné, elektronické či ústní formě třetí straně bez předchozího výslovného písemného souhlasu Smluvní strany, které se informace bezprostředně týká;

b) důvěrné informace nezneužít, nepoužít v rozporu s oprávněnými zájmy druhé Smluvní strany ve prospěch svůj nebo třetích osob a přijmout dostatečná opatření, aby se předešlo nepovolanému užívání důvěrných informací třetí stranou bez předchozího výslovného písemného souhlasu příslušné Smluvní strany;

c) poskytovat důvěrné informace výhradně pracovníkům, kteří se podílejí přímo na spolupráci a užití jejích výsledků a pouze k účelům, které jsou v souladu s účelem spolupráce a vedou přímo ke splnění jejích cílů;

d) nekopírovat důvěrné informace ani jiným způsobem je nereprodukovat bez výslovného souhlasu Smluvní strany, která je zpřístupnila, kromě užití pro konkrétní, Smluvními stranami stanovenou, interní potřebu Smluvních stran;

e) pokud mají informace zpřístupněné některou ze Smluvních stran druhé Smluvní straně charakter utajovaných informací chráněných zákonem o ochraně utajovaných informací nebo osobních údajů chráněných zákonem o ochraně osobních údajů a nařízením GDPR, je povinností dodržovat zásady stanovené příslušným zákonem. Každá ze Smluvních stran je rovněž povinna prokázat druhé Smluvní straně na její žádost, zda zákonem stanovené povinnosti dodržuje a jakým způsobem je jejich dodržování zajištěno.

14.10 Důvěrné informace, které budou v souladu s ustanoveními Smlouvy zpřístupněny druhé ze Smluvních stran „hmotnou formou“ (písemnou, elektronickou apod.), včetně jejich kopií, budou vráceny druhé straně nebo zničeny, jakmile:

a) bude ukončena spolupráce mezi Smluvními stranami;

b) Smluvní strana, která tyto důvěrné informace zpřístupnila, o to písemně požádá.

14.11 Poskytovatel je povinen zabezpečit veškeré podklady, mající charakter důvěrné informace, poskytnuté mu Resortem ŽP proti ztrátě, odcizení nebo jinému zneužití. Poskytovatel se zavazuje, že důvěrné informace užije pouze za účelem plnění ze Smlouvy. Jiná použití nejsou bez písemného svolení příslušného subjektu Resortu ŽP přípustná.

14.12 Poskytovatel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv Resortu ŽP nejméně ve stejném rozsahu, v jakém je v tomto závazkovém vztahu zavázán sám.

14.13 Povinnost zachovávat mlčenlivost dle tohoto článku Smlouvy, se nevztahuje na informace:

a) které je subjekt Resortu ŽP povinen poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;

b) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením ustanovení tohoto článku ze strany Poskytovatele;

c) které jsou Poskytovateli známy a byly mu volně k dispozici ještě před přijetím těchto informací od subjektu Resortu ŽP;

d) u nichž je Poskytovatel schopen prokázat, že mu byly známy ještě před přijetím těchto informací od subjektu Resortu ŽP, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů;

e) které budou Poskytovateli po uzavření Smlouvy sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána;

f) jejichž sdělení se vyžaduje ze ZZVZ.

14.14 Za prokázané porušení ustanovení v tomto článku Smlouvy má poškozená Smluvní strana právo požadovat náhradu takto vzniklé škody a vedle toho smluvní pokutu.

14.15 Závazky vyplývající z tohoto článku Smlouvy není Poskytovatel oprávněn vypovědět ani jiným způsobem jednostranně ukončit. Trvají i po ukončení Smlouvy.

Článek 15
Smluvní ujednání o zpracování osobních údajů

15.1 Smlouva je současně i smlouvou o zpracování osobních údajů ve smyslu § 6 zákona o ochraně osobních údajů a nařízení GDPR.

15.2 Subjekty Resortu ŽP mají pro účely ochrany osobních údajů postavení zpracovatele ve smyslu zákona o ochraně osobních údajů a nařízení GDPR a Poskytovatel má pro účely ochrany osobních údajů postavení správce ve smyslu těchto právních předpisů.

15.3 Resort ŽP je oprávněn zpracovávat osobní údaje za účelem plnění závazků ze Smlouvy a závazků vzniklých na jejím základě.

15.4 Resort ŽP je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění účelu Smlouvy, za tímto účelem je oprávněn zejména osobní údaje ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv Poskytovatele vyplývajících ze Smlouvy, předávat zpracované osobní údaje Poskytovateli, vše v souladu se zákonem o ochraně osobních údajů a nařízením GDPR.

Článek 16
Poddodavatelé

16.1 Pokud Poskytovatel prokázal v Zadávacím řízení, na jehož základě byla uzavřena Smlouva, splnění části kvalifikace prostřednictvím poddodavatele, musí tento poddodavatel plnit tu část jednotlivé služby, jež prokazoval za Poskytovatele. Jakákoliv změna poddodavatele Poskytovatele je možná pouze z vážných důvodů a za předpokladu doložení příslušné části kvalifikace obdobným způsobem novým poddodavatelem a po předchozím písemném souhlasu Centrálního zadavatele. Obdobně tomu bude v případě, že Poskytovatel ve své Nabídce uvedl, že část Veřejné zakázky bude plněna poddodavatelem.

16.2 V případě, že je předmět plnění či jakákoli jeho část plněna prostřednictvím poddodavatele, je Poskytovatel zavázán, jako by plnil sám.

Článek 17
Finanční kontrola a uchování dokumentace

17.1 Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů nebo z veřejné finanční podpory a je povinen poskytnout součinnost Objednateli i kontrolním orgánům při provádění finanční kontroly dle výše citovaného zákona o finanční kontrole.

17.2 Smluvní strany jsou povinny uchovávat veškerou dokumentaci související s realizací předmětu plnění dle Smlouvy včetně účetních dokladů po dobu 10 let od zániku závazků vyplývajících ze Smlouvy.

17.3 Poskytovatel je povinen kdykoliv na vyžádání poskytovat požadované informace a dokumentaci ohledně plnění Veřejné zakázky zaměstnancům nebo zmocněncům Objednatele a dalších pověřených orgánů (Ministerstvo financí, Nejvyšší kontrolní úřad, příslušný finanční úřad a případně další oprávněné orgány státní správy). Dále je Poskytovatel povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci Veřejné zakázky a poskytnout jim při provádění kontroly součinnost. Tyto povinnosti platí i pro poddodavatele a případné další osoby podílející se na realizaci Veřejné zakázky, přičemž Poskytovatel je povinen jejich součinnost a plnění povinností uvedených v tomto odstavci zajistit.

Článek 18
Závěrečná ustanovení

18.1 Smlouva a právní vztahy založené Smlouvou se řídí právním řádem České republiky. Práva a povinnosti Smluvních stran, pokud nejsou upraveny Smlouvou, se řídí zejména Občanským zákoníkem, ZZVZ a předpisy souvisejícími.

18.2 Veškeré případné spory vzniklé mezi Smluvními stranami na základě nebo v souvislosti se Smlouvou budou primárně řešeny jednáním Smluvních stran. V případě, že tyto spory nebudou v přiměřené době vyřešeny, budou k jejich projednání a rozhodnutí příslušné soudy České republiky.

18.3 V případě, že některé ustanovení Smlouvy je nebo se stane v budoucnu neplatným, neúčinným či nevymahatelným nebo bude-li takovým shledáno příslušným orgánem, zůstávají ostatní ustanovení Smlouvy v platnosti a účinnosti, pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž byla Smlouva uzavřena, nevyplývá, že jej nelze oddělit od ostatního obsahu Smlouvy. Smluvní strany se zavazují bezodkladně nahradit neplatné, neúčinné nebo nevymahatelné ustanovení Smlouvy ustanovením jiným, které svým obsahem a smyslem odpovídá nejlépe ustanovení původnímu a Smlouvě jako celku.

18.4 Smlouva může být, s výjimkou článku 8 odst. 8.9 Smlouvy, měněna nebo doplňována pouze formou písemných vzestupně číslovaných dodatků odsouhlasených a podepsaných oběma Smluvními stranami. Ke změnám či doplnění neprovedeným písemnou formou se nepřihlíží.

18.5 Poskytovatel není oprávněn postoupit práva ani převést povinnosti vyplývající ze Smlouvy na třetí osobu bez předchozího písemného souhlasu Centrálního zadavatele.

18.6 Poskytovatel se zavazuje, že v případě ukončení smluvního vztahu zajistí technickou podporu vydaných TSA minimálně po dobu jejich platnosti.

18.7 Smluvní strany na sebe přebírají nebezpečí změny okolností v souvislosti s právy a povinnostmi Smluvních stran vzniklými na základě Smlouvy. Smluvní strany vylučují uplatnění ustanovení § 1765 odst. 1, § 1766 a § 2620 Občanského zákoníku na svůj smluvní vztah založený Smlouvou.

18.8 Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami, resp. dnem podpisu druhé Smluvní strany a účinnosti dnem jejího uveřejnění v Informačním systému Registr smluv (dále jen „**ISRS**“) dle podmínek stanovených zejména zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Poskytovatel bezvýhradně souhlasí s uveřejněním celého znění Smlouvy v ISRS a na profilu Centrálního zadavatele (jakožto zadavatele Veřejné zakázky), popř. na dalších místech v souladu s příslušnými právními předpisy. Uveřejnění Smlouvy v ISRS provede Centrální zadavatel.

18.9 Smlouva se uzavírá ve 4 vyhotoveních, každý s platností originálu, přičemž Objednatel obdrží 2 vyhotovení a Poskytovatel rovněž 2 vyhotovení.

18.10 Nedílnou součástí Smlouvy jsou její přílohy:

a) Příloha č. 1: Centrální zadavatel a seznam Pověřujících zadavatelů;

b) Příloha č. 2: Realizační objednávka;

c) Příloha č. 3: Aktuální platné znění CPTSA Poskytovatele.

Smluvní strany prohlašují, že Smlouva vyjadřuje jejich svobodnou, vážnou, určitou a srozumitelnou vůli prostou omylu. Smluvní strany si Smlouvu přečetly, s jejím obsahem souhlasí, což stvrzují vlastnoručními podpisy.

Za Objednatele	**Za Poskytovatele**
V Praze, dne 13. 11. 2018	V Praze, dne 09. 11. 2018
Česká republika – Ministerstvo životního prostředí Ing. Jana Vodičková ředitelka odboru informatiky	**eldentity a. s.** Ing. Ladislav Šedivý předseda představenstva

Příloha č. 1: Centrální zadavatel a seznam Pověřujících zadavatelů

Česká republika – Ministerstvo životního prostředí

Vršovická 1442/65
100 10 Praha 1
Oprávněná osoba: Ing. František Zádrapa
Email: frantisek.zadrapa@mzp.cz
Telefon: +420 267 122 798

Česká republika – Agentura ochrany přírody a krajiny České republiky

Kaplanova 1931/1
148 00 Praha 11
Oprávněná osoba: Bc. Petr Kasal
Email: petr.kasal@nature.cz
Telefon: +420 283 069 311

CENIA, česká informační agentura životního prostředí

Vršovická 1442/65
100 10 Praha 10
Oprávněná osoba: Mgr. Miroslav Havránek
Email: miroslav.havranek@cenia.cz
Telefon: +420 267 125 226

Česká geologická služba

Klárov 131/3
118 21 Praha 1
Oprávněná osoba: Richard Binko
Email: richard.binko@geology.cz
Telefon: +420 257 089 435

Česká republika – Česká inspekce životního prostředí

Na Břehu 267
190 00 Praha 9
Oprávněná osoba: Jiří Hofman
Email: jiri.hofman@cizp.cz
Telefon: +420 773 774 310

Český hydrometeorologický ústav

Na Šabatce 2050/17
143 06 Praha 412 – Komořany
Oprávněná osoba: Ing. Ivo Durčanský
Email: durcansky@chmi.cz
Telefon: +420 244 032 606

Správa jeskyní České republiky

Květnové náměstí 3
252 43 Průhonice
Oprávněná osoba: Ing. Daniela Bílková
Email: bilkova@caves.cz
Telefon: +420 602 205 588, +420 271 000 042

Správa Krkonošského národního parku

Dobrovského 3
543 01 Vrchlabí
Oprávněná osoba: Mgr. Luděk Khol
Email: lkhol@krnap.cz
Telefon: +420 499 456 612, +420 737 217 101

Správa Národního parku České Švýcarsko

Pražská 52
407 46 Krásná Lípa
Oprávněná osoba: Ing. Pavel Benda, Ph.D.
Email: p.benda@npcs.cz
Telefon: +420 412 354 050, +420 737 276 998

Správa Národního parku Šumava

1. máje 260
385 01 Vimperk
Oprávněná osoba: Ing. Martin Roučka
Email: martin.roucka@npsumava.cz
Telefon: +420 731 530 208

Správa Národního parku Podyjí

Na Vyhlídce 5
669 01 Znojmo
Oprávněná osoba: Bc. Martin Kouřil
Email: kouril@nppodyji.cz
Telefon: +420 724 256 182

Státní fond životního prostředí České republiky

Olbrachtova 2006/9
140 00 Praha 4
Oprávněná osoba: Jan Smrčina
Email: jan.smrcina@sfzp.cz
Telefon: +420 267 994 352

Výzkumný ústav Silva Taroucy pro krajinu a okrasné zahradnictví, v.v.i.

Květnové nám. 391
252 43 Průhonice
Oprávněná osoba: Ing. Petr Seifert
Email: seifert@vukoz.cz
Telefon: +420 605 205 971

Výzkumný ústav vodohospodářský T. G. Masaryka, v.v.i.

Podbabská 2582/30
160 00 Praha 6
Oprávněná osoba: Ing. Vlastimil Mareš
Email: vlastimil.mares@vuv.cz
Telefon: +420 220 197 368

Příloha č. 2: Realizační objednávka

REALIZAČNÍ OBJEDNÁVKA

č. XY ze dne XX. YY. ZZZZ

pro plnění Smlouvy o poskytování časových razítek

(evidenční číslo přidělené z Centrální evidence smluv: 170217)

Objednatel:	.....
Se sídlem:	.....
IČO:	.....
Jednající:	.....
Bankovní spojení:	.....
Číslo účtu:	.....
Zástupce pro věcná jednání:	.....

Vymezení a popis požadovaného plnění (předpokládaný počet TSA):

.....

Doba a místo plnění:

Sídlo:	.....
Kontaktní osoba:	.....
Email:	.....
Telefon:	.....

Doplňující požadavky Objednatele:

.....

Jméno a podpis Oprávněné osoby:

.....

Příloha č. 3: Aktuální platné znění CPTSA Poskytovatele

(následuje)

Kvalifikovaný poskytovatel služeb vytvářejících důvěru eldentity a.s.

ACAeID 10.4 Certifikační politika - TSA

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

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	Zapracování připomínek auditu a dozorového orgánu
	17. 10. 2017	Michal Příhoda	Aktualizace v souvislosti s novými klíči a root certifikátem

OBSAH

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 stanping 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 zkratek

Zákon	Zákon 297/2016 Sb. o službách vytvářejících důvěru
ACAeID, ACA	Informační systém eIdentity 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	Zákon č. 297/2016 Sb. o službách vytvářejících důvěru, v platném
Z300	Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů
FIPS	Federal Information Processing Standards, mezinárodně respektovaný standardizační orgán USA
Nařízení eIDAS	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 pečetí
Veřejný klíč	Data pro ověřování elektronických podpisů nebo pečetí

Seznam použitých pojmů a zkratek

Revokace	zneplatnění certifikátu
Hash	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 eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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

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 pečetí 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 předpisech.

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 pečetí celého příslušného certifikačního řetězce.

Spoléhající se strana zváží, 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.

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
DIĆ: 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 směrnicí 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 pečetí 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 pečetí 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 pečetí)

6.2.2.1 Standardy a podmínky používání kryptografického modulu

Soukromé klíče, sloužící pro vytváření elektronických pečetí 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 pomocí 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 eIdentity 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)	eIdentity 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 žádající 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 nevydá.

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

Kavlifikované 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

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 pečetí 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	

Žádosti, 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 PKIStauts 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	
accurancy		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 nevydá.

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 provedeného 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 eIdentity 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 neoddělitelnou součástí práce všech vedoucích pracovníků eIdentity a.s. Personální bezpečnost eIdentity a.s. vnímá jako součást řádné správy společnosti, neboť je vyjádřením péče o svěřená aktiva.

Personální bezpečnost v oblasti ochrany citlivých aktiv tedy eIdentity 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 eIdentity a.s. označuje souhrn všech postupů, které vedou k ověření důvěryhodnosti zaměstnanců a k jejich vzdělávání vedoucímu 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 eIdentity 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 eIdentity 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 službě 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 prostupný 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 eIdentity 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, eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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 přiloženém 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 prohlížecí 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 eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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 eldentity 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 eldentity 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 eldentity 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 eIdentity a.s. zastupována třetí stranou. V takovém případě je mezi tímto zástupcem a společností eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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 eIdentity 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.