


Číslo Rámcové dohody MV-55917-43/VZ-2017
Číslo Rámcové dohody Poskytovatele: D2017101601

Rámcová dohoda na zajištění služeb vydávání elektronických časových razítek kvalifikovaným poskytovatelem služeb vytvářejících důvěru 2017-2021


uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „Občanský zákoník“) a v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, jakož i s dalšími zvláštními právními předpisy upravujícími závazné podmínky ve vztahu k předmětu plnění veřejné zakázky

(dále jen „**Rámcová dohoda**“)

Česká republika – Ministerstvo vnitra

Sídlo: Praha 7, Nad Štolou 3, PSČ 170 34
Jejímž jménem jedná: Mgr. Tomáš Kroupa, pověřen řízením odboru provozu informačních technologií a komunikací, na základě pověření ministrem vnitra ze dne 16. června 2017, č. j. MV-60864-1/SIK5-2017
IČO: 00007064
DIČ: CZ00007064
Bankovní spojení: 
Číslo účtu:
Kontaktní adresa:
(dále jen „**Centrální zadavatel**“)

Disig, a.s.

Sídlo: Bratislava, Záhradnícka 4871/151, PSČ 821 08, Slovenská republika
Jehož jménem jednají: Ing. Ľuboš Batěk – předseda představenstva
Ing. Ivan Kühn – podpředseda představenstva
IČO: 35975946
DIČ: SK2022116976
Bankovní spojení: 
Číslo účtu:
BIC (SWIFT):
(dále jen „**Poskytovatel**“)

(dále také společně označováni jako „**Smluvní strany**“). Za Smluvní stranu jsou v kontextu Rámcové dohody považovány též jednotlivé subjekty resortu MV/objednatelé – fakturační místa oprávněná požadovat na Poskytovateli plnění na základě Rámcové dohody za podmínek v ní stanovených.

I.

Základní pojmy

Pro účely Rámcové dohody se rozumí:

Ministerstvem vnitra („MV“) – centrální zadavatel a další organizační útvary začleněné v organizační složce MV, které jsou oprávněny na účet MV požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem Rámcové dohody za podmínek v ní stanovených;

Centrálním zadavatelem – organizační útvar MV České republiky, který je oprávněn jménem organizační složky státu MV a jménem pověřujících veřejných zadavatelů uvedených v příloze č. 1 Rámcové dohody v souladu s právními a vnitřními předpisy nebo na základě písemné Smlouvy o vymezení práv a povinností uzavřít Rámcovou dohodu a požadovat na Poskytovateli plnění ve formě služeb, které jsou jejím předmětem za podmínek v ní stanovených;

Pověřujícím veřejným zadavatelem – právní subjekt uvedený v příloze č. 1 Rámcové dohody, který uzavřel s Centrálním zadavatelem Smlouvu o vymezení práv a povinností a který je oprávněn na svůj účet požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem Rámcové dohody za podmínek v ní stanovených;

Smlouvou o vymezení práv a povinností – smlouva uzavřená před zahájením centralizovaného zadávání podle Rámcové dohody mezi Centrálním zadavatelem a jednotlivými pověřujícími veřejnými zadavateli, v níž si tyto Smluvní strany upravily svá vzájemná práva a povinnosti v souvislosti s centralizovaným zajištěním služeb kvalifikovaným poskytovatelům služeb vytvářejících důvěru;

Resortem MV – množina subjektů MV a pověřujících veřejných zadavatelů v rozsahu přílohy č. 1 Rámcové dohody;

Objednatel - fakturačním místem – subjekt resortu MV, oprávněný k zadání veřejné zakázky formou vystavení žádosti na základě Rámcové dohody, tj. oprávněný na účet MV nebo na svůj účet požadovat na Poskytovateli plnění ve formě služeb, které jsou předmětem Rámcové dohody 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 MV;

Poskytovatelem se rozumí – kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikovaná elektronická časová razítka nebo kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající elektronická časová razítka, včetně vydávání osobních i serverových komerčních autentizačních certifikátů pro zajištění služeb spojených s poskytováním časových razítek.

Seznam použitých zkratk:

TSA – kvalifikovaná elektronická časová razítka / elektronická časová razítka

KC – komerční osobní certifikát

KSC – komerční serverový certifikát

CPTSA – certifikační politika pro vydávání kvalifikovaných el. časových razítek / elektronických časových razítek

CPKC – certifikační politika pro komerční osobní certifikáty

CPKSC – certifikační politika pro komerční serverové certifikáty

SLA – dohoda o úrovni poskytovaných služeb

II.

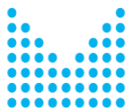
Účel dohody

1. Účelem Rámcové dohody je upravit podmínky týkající se poskytování opakujících se služeb, které jsou předmětem plnění dle Rámcové dohody, zadávaných po dobu její platnosti a zajistit tak vydávání TSA pro potřeby resortu MV plně v souladu s jeho potřebami, záměry, projekty a platnými zákonnými úpravami prostřednictvím Poskytovatele.
2. Poskytovatel prohlašuje, že disponuje všemi příslušnými oprávněními k podnikání a veškerými technickými, ekonomickými i personálními předpoklady nezbytnými pro řádné plnění předmětu Rámcové dohody. Poskytovatel 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.

III.

Předmět dohody

1. Předmětem Rámcové dohody jsou plnění realizována na jejím základě s cílem komplexního zajištění 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 („eIDAS“), resp. zákonem č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce, pro potřeby resortu MV 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 MV, a to zejména z důvodu změny legislativy či technologie, které mohou tyto požadavky na změny vyvolat. Požadavky na změny oznámí Poskytovatel Centrálnímu zadavateli nejpozději 10 pracovních dní před jejich zavedením.

2. TSA podle Rámcové dohody budou Poskytovatelem vydávána pouze oprávněnému žadateli.
3. Předmětem Rámcové dohody je současně zajištění autentizačních certifikátů ke službě TSA pro potřeby resortu MV, což zahrnuje zejména vydávání KC a KSC (pod označením KC a KSC se rozumí také přístupový token X.509) podle příslušných Certifikačních politik Poskytovatele, tj. CPKC a CPKSC, jejichž aktuální znění je uvedeno na webu Poskytovatele eidas.disig.sk/sk/documents/. Certifikáty budou vydávány prostřednictvím veřejných registračních autorit Poskytovatele, jejichž seznam je dostupný na eidas.disig.sk/sk/ralist či prostřednictvím výjezdu mobilní registrační autority Poskytovatele a to vždy a pouze na základě řádné žádosti doložené příslušnými dokumenty specifikovanými Rámcovou dohodou. Cena těchto autentizačních certifikátů je zahrnuta v cenách za poskytnutí služby TSA a tvoří její nedílnou součást.
4. Přehled a specifikace dokumentů, včetně jejich dodatků, potřebných pro vystavení autentizačních certifikátů jsou uvedeny v příloze č. 2 Rámcové dohody „**Přehled dokumentů**“ v rozpisu podle jednotlivých druhů certifikátů.
5. KC vydaným pro potřeby resortu MV se rozumí certifikát ve smyslu CPKC, u něhož je kromě totožnosti oprávněného žadatele ověřován také jeho zaměstnanecký poměr k subjektu resortu MV, který je Objednatelem - fakturačním místem.
6. Elektronické žádosti o komerční certifikáty musí splňovat naplnění položky jedinečného jména O, popřípadě OU a T, uvedené v dokladu stvrzujícím zaměstnanecký poměr.
7. Položka „O“ = název organizace – subjektu resortu MV je vždy naplněna zněním, kde seznam nabývaných hodnot této položky je odvozen od přílohy č. 1 a musí souhlasit vždy s obsahem, uvedeným v dokladu stvrzujícím zaměstnanecký poměr.
8. Údaje „OU“ = název organizační jednotky a „T“ = pozice v organizaci jsou nepovinné a jejich případné využití a obsah závisí na oprávněném žadateli, kterému má být certifikát vydán. Obsah položek „O“, „OU“ a „T“ musí vždy souhlasit s obsahem, uvedeným v dokladu stvrzujícím zaměstnanecký poměr.
9. KSC pro potřeby resortu MV budou vydávány při splnění požadavků daných platnou CPKSC a naplnění položky musí být vždy shodné s Žádostí o KSC – dokladem stvrzujícím položky uvedené v certifikátu.



IV.

Oprávněné osoby

1. Jednotlivé Doklady předkládané podle přílohy č. 2 Rámcové dohody „**Přehled dokumentů**“ jsou jménem subjektů resortu MV uvedených v příloze č. 1 Rámcové dohody (objednatelů) oprávněni podepisovat představení, služební funkcionáři nebo vedoucí zaměstnanci (dále jen “vedoucí“) oprávněni k zastupování příslušného subjektu MV nebo jimi zmocněné osoby (dále jen „Oprávněná osoba“).
2. Centrální zadavatel se zavazuje za resort MV vytvořit a předat Poskytovateli seznam oprávněných osob Objednatelů podle odstavce 1 nejpozději sedmi (7) dní přede dnem zahájení plnění podle Rámcové dohody.
3. Centrální zadavatel je oprávněn z vlastního podnětu nebo jemu adresovaných podnětů subjektů resortu MV v případě potřeby jednostranně seznam oprávněných osob měnit, včetně jeho rozšíření. Veškeré změny v seznamu oprávněných osob musí být dostatečně transparentní a musí být patrné, 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 Centrálního zadavatele, předané na adresu sídla Poskytovatele nebo na emailovou adresu [REDACTED] nejpozději 2 pracovní dny před datem požadované změny.

V.

Závazky resortu MV

1. Resort MV se zavazuje ve svých projektech využívajících TSA, vydaná jako plnění na základě Rámcové dohody, zabezpečit dodržování platné CPTSA Poskytovatele, jejíž aktuální znění je uvedeno na webu Poskytovatele eidas.disig.sk. Veškeré změny a doplňky tohoto dokumentu jsou vůči resortu MV účinné okamžikem předání změn a doplňků na e-mailovou adresu: [REDACTED]. Tyto změny a doplňky však nemají vliv na obsah dohody o předmětu a ceně plnění dle Rámcové dohody.
2. Centrální zadavatel se zavazuje jménem resortu MV, že při používání autentizačních certifikátů ke službě TSA, vydaných na základě Rámcové dohody, budou dodržovány CPKC a CPKSC Poskytovatele platné ke dni nabytí účinnosti Rámcové dohody.
3. Veškeré změny a doplňky CPKC a CPKSC, zaslané Poskytovatelem na e-mailovou adresu [REDACTED] jsou vůči resortu MV účinné okamžikem potvrzení ze strany Centrálního zadavatele, které učiní do 3 dnů od jejich obdržení, aniž by bylo nutné měnit Rámcovou dohodu. Tyto změny




a doplňky jsou také uveřejněny na  a nemají vliv na obsah dohody o předmětu a ceně plnění dle Rámcové dohody.

VI.

Závazky Poskytovatele

1. Poskytovatel zajišťuje plnění formou služby specifikované Rámcovou dohodou v souladu se závazným prohlášením v jejím článku II. odst. 2. Poskytovatel se zavazuje poskytovat jednotlivým subjektům resortu MV jako oprávněným žadatelům o služby časové autority danou službu pro jimi realizovaná řešení v souladu s platnou CPTSA Poskytovatele.
2. Poskytovatel se zavazuje poskytovat resortu MV podporu zaručenou platnou CPTSA.
3. 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 Rámcové dohody. Do doby 0,5 % možné nedostupnosti nejsou zahrnuty plánované a ohlášené odstávky služby (v délce maximálně 4 hodin v mimopracovní době 22:00 – 06:00 či ve dnech pracovního volna a státem uznaných svátcích), jež je Poskytovatel povinen ohlásit subjektům resortu MV nejméně 7 dní předem. Maximální jednorázová doba nedostupnosti činí maximálně 30 minut. Poskytovatel je dále povinen pravidelně kontrolovat, zda je systém vydávání TSA nakonfigurován podle požadavků platných zákonných úprav.
4. Poskytovatel se zavazuje poskytovat pověřeným osobám Centrálního zadavatele měsíční statistiky odběru TSA, a to v členění podle jednotlivých Objednatelů – fakturačních míst a Oprávněných žadatelů autentizujících se ke službě odběru TSA z přístupových míst definovaných Centrálním zadavatelem vždy za uplynulý kalendářní měsíc do 10. dne měsíce následujícího. Počet přístupových míst není omezen. Poskytovatel se zavazuje ve shodné lhůtě poskytovat pověřeným osobám objednatele – fakturačního místa měsíční statistiky odběru TSA, a to v členění podle jednotlivých Oprávněných žadatelů autentizujících se ke službě odběru TSA.
5. Poskytovatel se zavazuje poskytovat službu TSA s minimální propustností 10ks TSA/s.
6. 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
 - f) v případě, kdy poskytovatel vydává elektronická časová razítka, musí nejpozději do konce dubna 2018 začít vydávat kvalifikovaná elektronická časová razítka.
7. KC pro autorizaci ke službě TSA budou vydávány Oprávněnému žadateli v souladu s platnou CPKC po předložení:
- a) dokladů totožnosti;
 - b) dokumentů (viz příloha č. 2 „**Přehled dokumentů**“);
 - c) předložení elektronické žádosti o vydání komerčního certifikátu, jejíž naplnění položek odpovídá Článku III. bodu 6., 7. a 8. této Rámcové dohody.
8. KSC pro autorizaci ke službě TSA budou vydávány při splnění požadavků daných platnou CPKSC.
9. Poskytovatel ručí za jedinečnost identifikačních údajů Oprávněného žadatele uvedených v certifikátech vydaných podle Rámcové dohody.
10. Poskytovatel nebude akceptovat žádosti o vydání KC a KSC, které nesplňují náležitosti žádosti o certifikát podle Rámcové dohody.
11. Poskytovatel se zavazuje poskytovat Oprávněným žadatelům o KC podporu zaručenou CPKC a žadatelům o KSC podporu zaručenou CPKSC.
12. Poskytovatel se zavazuje zveřejňovat na své internetové stránce  seznam zneplatněných KC a zneplatněných KSC (dále jen „CRL“) v intervalu ne delším, než každých 24 hodin.

VII.

Přerušení poskytování služby

1. Poskytovatel je oprávněn přerušit poskytování služby vydávání TSA v případě zjištění, že došlo k narušení bezpečnosti nebo ztrátě integrity, jež má významný dopad na poskytování služby TSA, na základě soudního příkazu nebo v případě, že subjekty resortu MV budou závažným způsobem porušovat povinnosti vyplývající z Rámcové dohody.
2. Poskytovatel je povinen bez zbytečného odkladu vyrozumět resort MV o přerušení poskytování služby vydávání TSA způsobené narušením bezpečnosti

nebo ztrátou integrity, jež má významný dopad na poskytování služby TSA dle odstavce 1.

3. Přerušeni poskytování služby vydávání TSA z důvodů uvedených v odstavci 1 budou ukončena bezprostředně poté, co zanikly důvody, které k přerušeni poskytování služby vedly.

VIII.

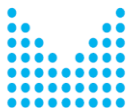
Cenové podmínky

1. Cena za vydání TSA je stanovena za jeden kus TSA. V takto stanovené ceně je již zohledněna cena za vydání autorizačních komerčních certifikátů.
2. Cena bude stanovena jako součin skutečně odebraného počtu TSA v příslušném kalendářním měsíci a ceny bez DPH za jeden kus TSA. K ceně bude připočteno DPH podle aktuálně platných předpisů.
3. Celková měsíční cena bude rozúčtována (vyfakturována) jednotlivým Objednatelům – fakturačním místům resortu MV podle jimi skutečně odebraného počtu v daném měsíci.
4. Cena za vydání jednoho TSA činí:
0,06,- Kč bez DPH + DPH v aktuální zákonné výši, jejíž sazba k datu uzavření Rámcové dohody činí 21%; cena s DPH za vydání jednoho kvalifikovaného časového razítka k datu podpisu Rámcové dohody tak činí 0,0726,- Kč.
5. Poskytovatel je povinen monitorovat stav plnění Rámcové dohody a informovat Centrálního zadavatele, pokud výše finančního čerpání přesáhne hodnotu 80% výše stanovené článkem IX. odstavce 6 Rámcové dohody.

IX.

Místa a doba plnění a způsob poskytování předmětu plnění

1. Místa plnění Objednatele jsou všechna místa uvedená v příloze č. 1 této Rámcové dohody.
2. Předmět plnění dle této Rámcové dohody bude Poskytovatelem zajišťován průběžně a to na základě Prováděcích smluv, které budou za Objednatele ve smyslu článku IV. odstavce 1 uzavírat jím pověřené Oprávněné osoby.
3. Prováděcí smlouva bude obsahovat minimálně následující náležitosti:
 - a. Identifikační údaje Objednatele a Poskytovatele
 - b. Číslo Prováděcí smlouvy
 - c. Způsob/zásady poskytování služby TSA
 - d. Místo plnění
 - e. Oprávněné osoby Objednatele a Poskytovatele

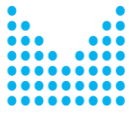


4. Smluvní strany berou na vědomí, že práva a povinnosti smluvních stran Prováděcí smlouvou neupravené, odpovídají právům a povinnostem Objednatele a Poskytovatele stanovených Rámcovou dohodou.
5. Prováděcí smlouvy budou uzavírány minimálně ve třech stejnopisech, kdy jeden z nich bude Poskytovatelem vždy nejpozději do třech dní od uzavření této Prováděcí smlouvy zaslán Centrálnímu zadavateli.
6. Celková hodnota všech plnění, která hodlá resort MV na základě Rámcové dohody pořídit, se bude odvíjet od skutečně poskytnutých služeb TSA až do výše celkové nabídkové ceny 3 000 000,- Kč (slovy: tři milióny korun) bez DPH.

X.

Platební podmínky

1. Úhrady ceny poskytnutých certifikačních služeb budou prováděny samostatně jednotlivými Objednateli - fakturačními místy definovanými v článku IX. odst. 1 a 2 Rámcové dohody, a to měsíčně zpětně za certifikační služby odebrané v předchozím kalendářním měsíci na základě Poskytovatelem vystaveného daňového dokladu (dále také „faktura“).
2. Faktura bude Objednateli - fakturačnímu místu vystavena a doručena podle skutečně dodaného objemu certifikačních služeb pro daného Objednatele - fakturační místo za uplynulý kalendářní měsíc do 10 dnů po datu uskutečnění zdanitelného plnění, kterým je poslední den příslušného kalendářního měsíce.
3. Ceny budou uvedeny s DPH, samostatně DPH a její sazba a ceny bez DPH.
4. Splatnost řádně vystavené faktury, činí 30 dnů od doručení Objednateli-fakturačnímu místu. Pokud bude takto vystavená faktura doručena subjektu resortu MV v období mezi 10. prosincem a 28. únorem roku následujícího, Smluvní strany se dohodly, že Poskytovatel prodlouží splatnost faktury na 60 kalendářních dní ode dne doručení. Veškeré platby podle Rámcové dohody budou probíhat výlučně bezhotovostním převodem v české měně. Za den úhrady faktury se považuje den podepsání příslušné částky z účtu Objednatele – fakturačního místa ve prospěch účtu Poskytovatele.
5. Překročení smluvených cen uvedených v čl. VIII. Rámcové dohody se nepřipouští.
6. Cenu je možné změnit pouze v případě, že dojde v průběhu realizace Rámcové dohody ke změnám daňových předpisů, upravujících výši DPH a to v rozsahu aktuální zákonné výše DPH.
7. Právo fakturovat předmět plnění vzniká po převzetí měsíčního přehledu odebraných časových razítek a jeho potvrzení oprávněným zástupcem Objednatele-fakturačního místa v místě plnění.
8. Vystavený daňový doklad/faktura musí obsahovat:
 - a) předmět plnění přesně dle Rámcové dohody;



- b) uvedení ceny;
 - c) číslo Rámcové dohody a Prováděcí smlouvy obou smluvních stran, úplné bankovní spojení Poskytovatele, zejména pak číslo účtu;
 - d) veškeré náležitosti dle § 29, odstavec 1, zákona č. 235/2004 Sb., o dani z přidané hodnoty (dále jen „ZDPH“), ve znění pozdějších předpisů;
 - e) náležitosti obchodní listiny ve smyslu ustanovení § 435 občanského zákoníku;
 - f) nedílnou součástí faktury (v příloze) bude měsíční přehled odebraných TSA, který musí obsahovat jednoznačné označení plnění včetně jednotkové a celkové ceny. Tento přehled je možno přiložit i v elektronické podobě.
9. Objednatel - fakturační místo má právo fakturu - daňový doklad Poskytovateli před uplynutím lhůty splatnosti vrátit, aniž by došlo k prodloužení s její úhradou, obsahuje-li faktura nesprávné údaje, nesprávné náležitosti požadované ve smlouvě, chybí-li na daňovém dokladu – faktuře některá z náležitostí, chybí-li originál dodacího dokladu, nebo obsahuje-li jiné cenové údaje nebo jiný druh či množství předmětu plnění než dohodnutý v Rámcové dohodě a oprávněně vykázaný v měsíčním přehledu odebraných TSA. Nová lhůta splatnosti v délce 30 dnů počne plynout ode dne doručení opraveného daňového dokladu Objednateli - fakturačnímu místu.
10. Daň z přidané hodnoty bude účtována v souladu se zákonnou úpravou platnou ke dni uskutečnění zdanitelného plnění.
11. Změnu výše DPH v rozsahu aktuální zákonné výše DPH ke dni uskutečnění zdanitelného plnění nelze považovat za změnu dohodnutých cen, pokud dojde v průběhu realizace Rámcové dohody ke změnám daňových předpisů, upravujících výši DPH.
12. Platby budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje budou uvedeny v této měně.
13. Poskytovatel se zavazuje, že nedojde k duplicitnímu plnění dle Rámcové dohody a jiných smluvních vztahů uzavřených s resortem MV.
14. Poskytovatel se zavazuje, že bankovní účet jím určený a uvedený v Rámcové dohodě a uzavřených Prováděcích smlouvách pro zaplacení jakéhokoliv závazku na základě Rámcové dohody bude od data podpisu Rámcové dohody do ukončení platnosti závazků z ní plynoucích zveřejněn způsobem umožňující dálkový přístup ve smyslu § 96 odst. 2 ZDPH.
15. Pokud Objednateli vznikne podle § 109 ZDPH ručení za nezaplacenou DPH z přijatého zdanitelného plnění od Poskytovatele, nebo se Objednatel důvodně domnívá, že tyto skutečnosti nastaly nebo mohly nastat, má Objednatel právo bez souhlasu Poskytovatele uplatnit postup zvláštního způsobu zajištění daně, tzn., že je Objednatel oprávněn odvést částku DPH podle faktury vystavené

Poskytovatelem přímo příslušnému finančnímu úřadu a to v návaznosti na § 109 a § 109a) ZDPH.

XI.

Dodání předmětu plnění

1. 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 Evropské unie.
2. Předmět plnění musí vyhovovat bezpečnostním standardům, jejichž použití je obvyklé u obdobných produktů, a musí svou technickou úroveň odpovídat podmínkám resortu MV v oblasti bezpečnosti a provozu informačních a komunikačních technologií.

XII.

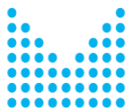
Oprávnění zástupci a komunikace smluvních stran

1. Oprávněnou osobou za resort MV pro věcná plnění dle Rámcové dohody je ředitel centrálního zadavatele, případně další osoby jím pověřené.
2. Oprávněné osoby Poskytovatele pro věcná plnění dle Rámcové dohody jsou zástupci jeho statutárních orgánů, případně osoby pověřené statutárním orgánem Poskytovatele.
3. Jména oprávněných osob Centrálního zadavatele a Poskytovatele označená jako Seznam oprávněných osob pro věcná plnění dle Rámcové dohody si smluvní strany navzájem písemně oznámí do sedmi (7) pracovních dní ode dne nabytí účinnosti Rámcové dohody.
4. Změny v Seznamu oprávněných osob centrálního zadavatele a Poskytovatele pro věcná plnění dle Rámcové dohody si smluvní strany písemně oznámí nejpozději do sedmi (7) pracovních dní ode dne uskutečnění této změny. Pro provedení změny platí zásady uvedené v odstavci 1 a 2 tohoto článku.
5. Centrální zadavatel současně předá Poskytovateli za resort MV seznam osob oprávněných za jednotlivé objednatele – fakturační místa podepsat/potvrdit správnost měsíčního přehledu odebraných TSA.

XIII.

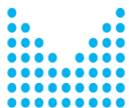
Odpovědnost za škodu, smluvní pokuty a úrok z prodlení

1. Poskytovatel odpovídá Centrálnímu zadavateli a jednotlivým Objednatelům - fakturačním místům za škodu způsobenou při plnění závazků z Rámcové dohody v důsledku porušení povinností vyplývajících z obecně závazných právních předpisů či vyplývajících z Rámcové dohody. Odpovědnost za škodu způsobenou

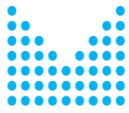


porušením smluvní povinnosti se řídí ustanovením § 2913 a násl. občanského zákoníku. Smluvní strany se zavazují vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.

2. Poskytovatel neodpovídá za škodu, která vznikla z důvodu nesprávného nebo neoprávněného využívání certifikačních služeb na straně resortu MV Poskytovatel neodpovídá za škodu způsobenou zejména:
 - a) porušením povinností, plynoucích resortu MV z Rámcové dohody;
 - b) jednáním nebo opomenutím třetí strany, dodávající resortu MV produkty nebo služby požadované v souvislosti s využíváním certifikačních služeb;
 - c) zaviněním resortu MV, jeho zaměstnanců, jeho zástupců nebo jeho smluvních partnerů.
3. Subjekt resortu MV nese plnou a výlučnou odpovědnost za jím zaviněné škody vzniklé Poskytovateli v souvislosti s nedodržením CPKC, CPKSC a CPTSA Poskytovatele.
4. Žádná Smluvní strana není povinna k náhradě škody, prokáže-li, že jí ve splnění povinnosti z Rámcové dohody dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání výše uvedených překážek.
5. Brání-li některé ze Smluvních stran v plnění povinností z Rámcové dohody mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 občanského zákoníku, je Smluvní strana, na jejíž straně překážka vznikla, povinna o vzniku, důsledcích, povaze a zániku takové překážky druhou Smluvní stranu neprodleně informovat. Zpráva musí být podána písemně, neprodleně poté, kdy se povinná Smluvní strana o překážce dozvěděla, nebo při náležitě 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, ke kompenzaci doby, která uplynula v důsledku takového prodlení. Pokud překážka nepomine do 3 pracovních dnů od doby svého vzniku, oprávnění zástupci obou Smluvních stran se sejdou za účelem projednání dalšího postupu při plnění závazků vyplývajících z Rámcové dohody.
6. 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.
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.
8. V případě překročení nedostupnosti 0,5% uvedené v článku VI. odst. 3 o více než 1 hodinu za kalendářní rok, je Poskytovatel povinen uhradit Centrálnímu zadavateli smluvní pokutu ve výši 10.000,- Kč. Za každou další hodinu nedostupnosti činí smluvní pokuta 20.000,- Kč.
 9. V případě nesplnění minimální propustnosti 10 ks TSA/s uvedené v článku VI. odst. 5 je Poskytovatel povinen uhradit Centrálnímu zadavateli smluvní pokutu ve výši 10.000,- Kč za takové porušení. Za další porušení je Poskytovatel povinen uhradit centrálnímu zadavateli smluvní pokutu ve výši 20.000,- Kč.
 10. V případě prodlení Poskytovatele s plněním povinností uvedených v článku VI. odst. 4 a 12 a článku X. odst. 2 Rámcové dohody v termínu vyplývajícím z Rámcové dohody či právních předpisů má příslušný subjekt resortu MV/objednatel – fakturační místo právo uplatnit vůči Poskytovateli smluvní pokutu ve výši 0,05 % (slovy: pět setin procenta) z celkové ceny měsíčního předmětu plnění včetně DPH za každý i započatý den prodlení.
 11. V případě, že některá ze Smluvních stran poruší některou z povinností, uložených článkem XIV. Ochrana informací, má druhá Smluvní strana právo účtovat smluvní pokutu ve výši 20.000 Kč za každý případ porušení.
 12. 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.
 13. Subjekt resortu MV/objednatel – fakturační místo je povinen zaplatit Poskytovateli za prodlení s úhradou faktury po sjednané lhůtě splatnosti úrok z prodlení ve výši 0,05% z dlužné částky, tj. oprávněně fakturované částky včetně DPH, podle příslušné faktury za každý, byť i započatý, den prodlení. Výše sankce není omezena.
 14. Vznikem povinnosti platit smluvní pokutu ani jejím faktickým zaplacením není dotčeno právo poškozené Smluvní strany na náhradu škody v plné výši ani právo odstoupit od této dohody. Odstoupením od Rámcové dohody nárok na již uplatněnou smluvní pokutu nezaniká.
 15. Žádná ze smluvních stran není odpovědná za prodlení svých závazků v rozsahu, v jakém je prodlení způsobeno prodlením s plněním závazků druhé Smluvní strany, zejména v případě neposkytnutí požadované součinnosti vymezené v Rámcové dohodě. Žádná ze Smluvních stran není povinna zaplatit smluvní pokutu, pokud prokáže, že porušení povinností bylo způsobeno mimořádnou nepředvídatelnou a nepřekonatelnou překážkou vzniklou nezávisle na vůli Smluvní strany ve smyslu § 2913 odst. 2 občanského zákoníku.
 16. Smluvní pokuty a úrok z prodlení jsou splatné do 30 kalendářních dnů po obdržení vyúčtování smluvní pokuty povinné Smluvní straně. Pokud bude takto



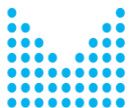
vystavená faktura doručena subjektu resortu MV jako povinné Smluvní straně v období mezi 10. prosincem a 28. únorem roku následujícího, Smluvní strany se dohodly, že Poskytovatel prodlouží splatnost faktury na 60 kalendářních dní ode dne doručení.

17. Zaplacením smluvní pokuty a úroku z prodlení není dotčen nárok Smluvních stran na náhradu škody v plném rozsahu. Trvá povinnost Poskytovatele dále řádně poskytovat plnění podle Rámcové dohody, pokud nedojde k jejímu zániku/ukončení.

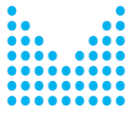
XIV.

Ochrana informací

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.
2. Dále je předmětem Rámcové dohody 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 a charakter osobních údajů dle ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Smluvní strany jsou si vzájemně rovněž povinny na žádost druhé Smluvní strany prokázat způsob, jakým je dodržování povinností stanovených příslušným zákonem zajištěno.
3. Smluvní strany budou považovat ve smyslu této Rámcové dohody za důvěrné:
 - a) informace poskytnuté ze strany resortu MV Poskytovateli v souvislosti s přípravou a realizací Rámcové dohody 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 zákona č. 134/2016 Sb., v platném znění.
 - d) utajované informace ve smyslu zákona č. 412/2005 Sb., ve znění pozdějších předpisů a osobní údaje ve smyslu zákona č. 101/2000 Sb., ve znění pozdějších předpisů informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti nebo informace o resortu MV, které by mohly z povahy věci být považovány za důvěrné a které se dozvědí v souvislosti s plněním Rámcové dohody.



4. 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 MV proti odcizení nebo jinému zneužití. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti po dobu 6 let po ukončení platnosti této Rámcové dohody, není-li zvláštním právním předpisem pro určitou skupinu informací stanovena lhůta delší.
5. Smluvní strany se zavazují chránit důvěrné informace druhé Smluvní strany v režimu obvyklé ochrany obchodního tajemství, není-li zvláštním právním předpisem stanoveno jinak.
6. Žádná ze Smluvních stran není oprávněna důvěrné informace podle Rámcové dohody, 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.
7. Smluvní strany jsou povinny vytvářet podmínky pro zabezpečení ochrany informací důvěrného charakteru a jejich ochranu zajistit.
8. Smluvní strany jsou oprávněny využívat důvěrné informace pouze a výhradně pro účely spolupráce vyplývající z Rámcové dohody a uzavřených Prováděcích smluv mezi nimi uzavřenými.
9. Smluvní strany jsou povinny zabezpečit, že povinnosti vyplývající z Rámcové dohody a budou dodržovány všemi zaměstnanci, pokud tito zaměstnanci získají nebo jsou jim k dispozici informace důvěrného charakteru.
10. 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



č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů nebo osobních údajů chráněných zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, 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.

11. Důvěrné informace, které budou v souladu s ustanoveními Rámcové dohody zpřístupněny druhé ze Smluvních stran „hmotnou formou“ (písemnou, elektronickou apod.), včetně jejich kopií, budou vráceny druhé straně nebo zničeny, jakmile:
 - a) bude ukončena spolupráce;
 - b) Smluvní strana, která tyto důvěrné informace zpřístupnila, o to požádá.
12. Poskytovatel je povinen zabezpečit veškeré podklady, mající charakter důvěrné informace, poskytnuté mu resortem MV proti ztrátě, odcizení nebo jinému zneužití. Poskytovatel se zavazuje, že důvěrné informace užije pouze za účelem plnění z Rámcové dohody. Jiná použití nejsou bez písemného svolení příslušného subjektu resortu MV přípustná.
13. Poskytovatel je povinen svého případného subdodavatele zavázat povinností mlčenlivosti a respektováním práv resortu MV nejméně ve stejném rozsahu, v jakém je v tomto závazkovém vztahu zavázán sám.
14. Povinnost zachovávat mlčenlivost dle tohoto článku, se nevztahuje na informace:
 - a) které je subjekt resortu MV 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 MV,
 - d) u nichž je Poskytovatel schopen prokázat, že mu byly známy ještě před přijetím těchto informací od subjektu resortu MV, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů,
 - e) které budou Poskytovateli po uzavření Rámcové dohody sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána,
 - f) jejichž sdělení se vyžaduje ze zákona.

15. Za prokázané porušení ustanovení v tomto článku má poškozená Smluvní strana právo požadovat náhradu takto vzniklé škody a vedle toho smluvní pokutu.
16. Smluvní strany berou na vědomí, že originál podepsané Rámcové dohody a uzavřených Prováděcích smluv bude v elektronické podobě zveřejněn na internetových stránkách Ministerstva vnitra a dle zákona o zadávání veřejných zakázek na profilu MV, a to bez časového omezení.
17. Závazky vyplývající z tohoto článku dohody není Poskytovatel oprávněn vypovědět ani jiným způsobem jednostranně ukončit. Trvají i po ukončení Rámcové dohody.

XV.

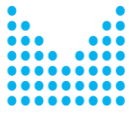
Smluvní ujednání o zpracování osobních údajů

1. Tato Rámcová dohoda je současně i smlouvou o zpracování osobních údajů ve smyslu § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a ve smyslu § 6 zákona.
2. Subjekty resortu MV mají pro účely ochrany osobních údajů postavení zpracovatele ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a Poskytovatel má pro účely ochrany osobních údajů postavení správce ve smyslu tohoto zákona.
3. Resort MV je oprávněn zpracovávat osobní údaje za účelem plnění závazků z Rámcové dohody a závazků vzniklých na jejím základě.
4. Resort MV je oprávněn zpracovávat osobní údaje v rozsahu nezbytně nutném pro plnění účelu Rámcové dohody, za tímto účelem je oprávněn zejména osobní údaje ukládat na nosiče informací, upravovat, uchovávat po dobu nezbytnou k uplatnění práv Poskytovatele vyplývajících z Rámcové dohody, předávat zpracované osobní údaje Poskytovateli, osobní údaje v případech stanovených Poskytovatelem nebo zákonem likvidovat.

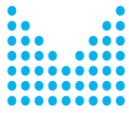
XVI.

Trvání a ukončení smluvního vztahu

1. Rámcová dohoda se uzavírá na dobu 4 roků (48 měsíců) nebo do vyčerpání nabídkové ceny uvedené v čl. IX bodu 6 této Rámcové dohody.
2. Smluvní vztah založený Rámcovou dohodou lze ukončit před jeho splněním v dohodnutém termínu:
 - a) písemnou dohodou Smluvních stran;
 - b) odstoupením Smluvních stran od Rámcové dohody v případech stanovených zákonem pro porušení dohody;



- c) odstoupením centrálním zadavatelem z důvodů stanovených Rámcovou dohodou, které vznikly po uzavření dohody na straně Poskytovatele;
 - d) výpovědí podanou podle § 1998 odst. 1 občanského zákoníku.
3. Pro případ ukončení Rámcové dohody dohodou Smluvních stran nastanou účinky ukončení Rámcové dohody k okamžiku stanovenému v takovéto dohodě.
4. Smluvní strany mohou Rámcovou dohodu vypovědět, stanoví-li tak zákon. Centrální zadavatel je oprávněn Rámcovou dohodu vypovědět písemnou výpovědí i bez udání důvodu. Rámcovou dohodu lze vypovědět s šestiměsíční (6) výpovědní lhůtou, která počíná běžet prvním dnem měsíce následujícího po dni doručení výpovědi druhé Smluvní straně.
5. Smluvní strany /Centrální zadavatel a Poskytovatel/ jsou oprávněny odstoupit od Rámcové dohody z důvodů uvedených v zákoně a dále z důvodů uvedených v Rámcové dohodě, zejména v případě podstatného porušení Rámcové dohody ve smyslu ustanovení § 2002 občanského zákoníku, pokud podstatné porušení Rámcové dohody, které je důvodem pro odstoupení, nebylo způsobeno okolnostmi vylučujícími odpovědnost dle ustanovení § 2913 odst. 2 občanského zákoníku.
6. Centrální zadavatel je oprávněn od Rámcové dohody odstoupit v následujících případech:
- a) bude rozhodnuto o ukončení činnosti (likvidaci) Poskytovatele;
 - b) Poskytovatel podá insolvenční návrh jako dlužník, insolvenční návrh podaný proti Poskytovateli bude zamítnut pro nedostatek majetku, bude rozhodnuto o úpadku Poskytovatele nebo bude ve vztahu k Poskytovateli vydáno jiné rozhodnutí s obdobnými účinky;
 - c) Poskytovatel bude odsouzen za úmyslný trestný čin;
 - d) Poskytovateli byla odebrána oprávnění, která jsou pro výkon jeho činnosti v návaznosti na poskytování předmětu Rámcové dohody vyžadována zákonem.
7. Za podstatné porušení Rámcové dohody Poskytovatelem, které je důvodem pro odstoupení centrálního zadavatele od Rámcové dohody, se považuje:
- a) Přerušování poskytování služby TSA o více jak 5 kalendářních dní;
 - b) realizace předmětu Rámcové dohody v rozporu s právními předpisy nebo Rámcovou dohodou;
 - c) jiné porušení povinností Poskytovatele, které nebude odstraněno do 10 kalendářních dní od doručení výzvy centrálního zadavatele Poskytovateli.
8. Za podstatné porušení Rámcové dohody ze strany resortu MV, které je důvodem pro odstoupení od Rámcové dohody Poskytovatelem, se považuje:



- a) prodlení MV s úhradou faktury – daňového dokladu o více jak 30 kalendářních dní, přičemž nárok na úrok z prodlení není tímto ustanovením dotčen;
 - b) prodlení MV s poskytnutím součinnosti o více než 30 kalendářních dní od prokazatelného doručení písemné výzvy ze strany Poskytovatele.
9. Centrální zadavatel má v případě odstoupení od Rámcové dohody nárok na náhradu škody spočívající v náhradě prokazatelných nákladů, které mu vzniknou v souvislosti se zajištěním náhradního plnění
10. Pro podstatné porušení Rámcové dohody může oprávněná Smluvní strana odstoupit od dohody bez zbytečného odkladu. Odstoupení musí mít písemnou formu, musí v něm být uveden odkaz na ujednání Rámcové dohody či ustanovení právních předpisů, které zakládá oprávnění od Rámcové dohody 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 dohody odstoupit druhé Smluvní straně.
11. Práva smluvních stran vzniklá před odstoupením od Rámcové dohody nejsou odstoupením dotčena.
12. Odstoupení od Rámcové dohody či jiné ukončení smluvního vztahu jí založeného (navazující Prováděcí smlouvy) se nedotýká nároku na náhradu škody, smluvních pokut, ochrany neveřejných informací, zajištění pohledávky kterékoliv ze stran, řešení sporů a ustanovení týkajících se těch práv a povinností, z jejichž povahy toto vyplývá. Nedotýká se nároků, práv a ujednání ve smyslu § 2005 odst. 2 občanského zákoníku.

XVII.

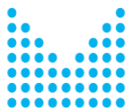
Rozhodné právo, řešení sporů

1. Rámcová dohoda se řídí právním řádem České republiky.
2. Veškeré spory mezi Smluvními stranami týkající se závazků z Rámcové dohody a závazků na jejím základě založených nebo jejího porušení, ukončení nebo neplatnosti, budou rozhodovány obecnými soudy České republiky.

XVIII.

Odpovědnost za vady

1. Poskytovatel prohlašuje, že předmět plnění dle Rámcové dohody je bez právních vad, zejména že není a nebude zatížen žádnými právy třetích osob, z nichž by pro resort MV 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 MV na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.

2. Poskytovatel po dobu platnosti a účinnosti Rámcové dohody a závazků z ní plynoucích odpovídá a ručí za to, že předmět plnění bude v souladu s Rámcovou dohodou 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 z Rámcové dohody.
3. Subjekt resortu MV je oprávněn kdykoliv v průběhu doby platnosti a účinnosti Rámcové dohody a závazků z ní plynoucích uplatnit vady předmětu plnění u Poskytovatele bez ohledu na to, kdy takové vady zjistil nebo mohl zjistit.
4. Poskytovatel nenese odpovědnost za neposkytnutí služby, za zhoršení její kvality nebo za zpoždění v jejím poskytnutí, pokud:
 - a) bude zaviněno jednáním nebo opomenutím subjektu resortu MV, jeho zaměstnanců nebo třetích osob jemu smluvně zavázaných;
 - b) vznikne v průběhu nutné plánované údržby nebo nutné odstávky systémů Poskytovatele nahlášené subjektu resortu MV nejméně 7 dní před termínem plánované údržby nebo nutné odstávky v souladu s postupy uvedenými v Rámcové dohodě;
 - c) bude způsobeno událostmi vyšší moci;
 - d) bude způsobeno přerušením služeb popsaným v čl. VII. Přerušení poskytování služby.

XIX.

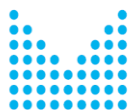
Změny dohody

Rámcovou dohodu lze měnit či doplňovat pouze dohodou Smluvních stran oprávněných k jejímu uzavření, a to písemnými dodatky takto označovanými a číslovanými vzestupnou řadou, podepsanými oprávněnými zástupci těchto Smluvních stran. Jiná ujednání jsou neplatná.

XX.

Zvláštní podmínky

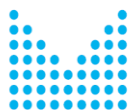
Poskytovatel se zavazuje, že v případě ukončení smluvního vztahu zajistí technickou podporu vydaných TSA minimálně po dobu jejich platnosti.



XXI.

Závěrečná ustanovení

1. Rámcová dohoda nabývá platnosti a účinnosti dnem uzavření rámcové dohody. (Popř. v době uzavření po 1. 7. 2017 bude účinná dnem uveřejnění v Registru smluv).
2. Poskytovatel není oprávněn postoupit práva ani převést povinnosti vyplývající z Rámcové dohody na třetí osobu bez předchozího písemného souhlasu Centrálního zadavatele.
3. V případě, že by některé ujednání Rámcové dohody bylo z jakýchkoliv důvodů neplatné či neúčinné, nezpůsobuje tato skutečnost neplatnost ani neúčinnost ostatních ujednání Rámcové dohody. Smluvní strany (Centrální zadavatel a Poskytovatel) se zavazují nahradit po vzájemné dohodě dotčené ustanovení jiným ustanovením, blížícím se svým účelem a obsahem nejvíce obsahu a účelu neplatného či neúčinného ustanovení.
4. Rámcová dohoda je vyhotovena v pěti (5) stejnopisech s platností originálu, z nichž strana Centrálního zadavatele obdrží tři (3) stejnopisy a strana Poskytovatele dva (2) stejnopisy. Centrální zadavatel zajistí distribuci kopie Rámcové dohody všem subjektům resortu MV, tak aby mohly řádně plnit závazky a uplatňovat práva jim z ní plynoucí.
5. Tato Rámcová dohoda bude uveřejněna v Registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.
6. Rámcová dohoda představuje úplnou dohodu Smluvních stran ohledně vzájemných vztahů, které upravuje, a nahrazuje veškerá předcházející ústní či písemná ujednání a dohody ve věcech upravených Rámcovou dohodou.



7. Seznam příloh, které tvoří nedílnou součást této Rámcové dohody:

Číslo přílohy	Název přílohy	Počet listů
Příloha č. 1	Seznam zadavatelů	2
Příloha č. 2	Certifikační politika TSA	27
Příloha č. 3	Specifikace poskytovaných služeb TSA	7
Příloha č. 4	Prováděcí smlouva a příloha	3 + 1

V Bratislavě dne 16.10.2017

V Praze dne

za Poskytovatele:
Ing. Lubos Batek
Digitally signed by Ing.
Lubos Batek
Date: 2017.10.17
14:10:07 +02'00'

.....
Ing. Ľuboš Batěk
předseda představenstva

Ing. Ivan Kuhn
Digitally signed by
Ing. Ivan Kuhn
Date: 2017.10.17
14:11:40 +02'00'

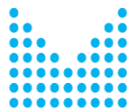
.....
Ing. Ivan Kühn
místopředseda představenstva

za Ministerstvo vnitra:
Mgr. Tomáš Kroupa
Digitálně podepsal
Mgr. Tomáš Kroupa
Datum: 2017.10.17
15:53:03 +02'00'

.....
Mgr. Tomáš Kroupa
pověřen řízením odboru provozu informačních
technologií a komunikací,
na základě pověření ministra vnitra

SEZNAM ZADAVATELŮ

1. Policejní akademie ČR v Praze
2. Vyšší policejní škola MV v Praze
3. Vyšší policejní škola a Střední policejní škola MV v Holešově
4. Muzeum Policie České republiky
5. Zdravotnické zařízení Ministerstva vnitra
6. Olymp Centrum sportu Ministerstva vnitra
7. Správa uprchlických zařízení Ministerstva vnitra
8. Krajské ředitelství policie hlavního města Prahy
9. Krajské ředitelství policie Středočeského kraje
10. Krajské ředitelství policie Jihočeského kraje
11. Krajské ředitelství policie Plzeňského kraje
12. Krajské ředitelství policie Karlovarského kraje
13. Krajské ředitelství policie Ústeckého kraje
14. Krajské ředitelství policie Libereckého kraje
15. Krajské ředitelství policie Královéhradeckého kraje
16. Krajské ředitelství policie Pardubického kraje
17. Krajské ředitelství policie Kraje Vysočina
18. Krajské ředitelství policie Jihomoravského kraje
19. Krajské ředitelství policie Olomouckého kraje
20. Krajské ředitelství policie Zlínského kraje
21. Krajské ředitelství policie Moravskoslezského kraje
22. Správa logistického zabezpečení Policejního prezidia ČR
23. Národní archiv
24. Státní oblastní archiv v Praze
25. Státní oblastní archiv v Třeboni
26. Státní oblastní archiv v Plzni
27. Státní oblastní archiv v Litoměřicích
28. Státní oblastní archiv v Zámrsku
29. Moravský zemský archiv v Brně
30. Zemský archiv v Opavě
31. Institut pro veřejnou správu Praha
32. Generální ředitelství Hasičského záchranného sboru ČR
33. Hasičský záchranný sbor hlavního města Prahy
34. Hasičský záchranný sbor Středočeského kraje
35. Hasičský záchranný sbor Jihočeského kraje
36. Hasičský záchranný sbor Plzeňského kraje
37. Hasičský záchranný sbor Karlovarského kraje
38. Hasičský záchranný sbor Ústeckého kraje
39. Hasičský záchranný sbor Libereckého kraje
40. Hasičský záchranný sbor Královéhradeckého kraje
41. Hasičský záchranný sbor Pardubického kraje
42. Hasičský záchranný sbor Kraje Vysočina
43. Hasičský záchranný sbor Jihomoravského kraje
44. Hasičský záchranný sbor Olomouckého kraje
45. Hasičský záchranný sbor Moravskoslezského kraje
46. Hasičský záchranný sbor Zlínského kraje



47. Záchranný útvar Hasičského záchranného sboru České republiky
48. Střední odborná škola PO a Vyšší odborná škola PO ve Frýdku-Místku
49. Bytová správa Ministerstva vnitra
50. Tiskárna Ministerstva vnitra
51. Zařízení služeb pro Ministerstvo vnitra
52. Odbor centrálních informačních systémů MV
53. Správa základních registrů
54. Generální inspekce bezpečnostních sborů



POLITIKA

poskytování důvěryhodné služby vyhotovování
kvalifikovaných elektronických časových
razítek



Disig, a.s.

Vypracoval



Datum platnosti

26. 7. 2017

Verze

4.1

Typ

POLITIKA

Schválil

Ing. Luboš Batěk

Obsah

1.	Úvod	4
1.1	Přehled	4
1.2	Název dokumentu a jeho identifikace	5
1.3	Účastníci PKI	5
1.3.1	Jednotka vyhotovování časových razítek	6
1.3.2	Registrační autorita	6
1.3.3	Zákazník	7
1.3.4	Spoléhající se strana	7
1.3.5	Jiní účastníci	7
1.4	Použitelnost časového razítka	8
1.5	Správa politiky	8
1.5.1	Organizace odpovědná za správu dokumentu	8
1.5.2	Kontaktní osoba	8
1.5.3	Osoba rozhodující o souladu CP s certifikační politikou	9
1.5.4	Postupy schvalování CP a externí politiky	9
1.6	Definice a zkratky	9
1.6.1	Definice	9
1.6.2	Zkratky	10
2.	Úložiště	11
2.1	Zveřejňování informací o TSA	11
2.2	Frekvence zveřejňování informací	11
2.3	Kontroly přístupu	11
3.	Obecná ustanovení	13
3.1	Obecná ustanovení politiky	13
3.2	Služby související s časovým razítkem	13
3.3	Vydavatel časových razítek	13
3.4	Uživatel časového razítka	13
4.	Úvod do politiky časového razítka a plnění obecných požadavků	14
4.1	Obecně	14
4.2	Cíloví uživatelé a použití	14
4.2.1	Správné praxe uplatňování politiky vyhotovování časových razítek	14
5.	Politiky a pravidla	15
5.1	Ohodnocení rizik	15
5.2	Pravidla pro praktický výkon důvěryhodných služeb	15

Soubor	CP_TSA_Disig	Verze	4.1
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017
		Strana	2/27

5.3	Všeobecné podmínky	15
5.4	Politika informační bezpečnosti	15
5.5	Závazky Poskytovatele	15
5.5.1	Obecně	15
5.5.2	Závazky Poskytovatele k Zákazníkovi	15
5.6	Informace pro spoléhající se strany	16
6.	Management a provoz TSA Poskytovatele	17
6.1	Úvod	17
6.2	Vnitřní organizace	17
6.3	Personální bezpečnost	17
6.4	Správa aktiv	17
6.5	Řízení přístupu	17
6.6	Kryptografické opatření	18
6.6.1	Obecně	18
6.6.2	Generování klíčů pro TSU	18
6.6.3	Ochrana soukromého klíče TSU	18
6.6.4	Certifikát veřejného klíče TSU	19
6.6.5	Přepsání klíče TSU	19
6.6.6	Management životního cyklu podpisového kryptografického hardwaru	19
6.6.7	Ukončení životního cyklu klíče TSU	19
6.7	Provedení časového razítka	20
6.7.1	Vydání časového razítka	20
6.7.2	Synchronizace hodin s UTC	21
6.8	Fyzická a objektová bezpečnost	21
6.9	Provozní bezpečnost	22
6.10	Síťová bezpečnost	22
6.11	Řízení bezpečnostních incidentů	23
6.12	Sběr důkazů	23
6.13	Řízení kontinuity činnosti organizace	23
6.14	Ukončení činnosti Poskytovatele a plány ukončení činnosti	24
6.15	Shoda	24
7.	Plnění požadavků pro kvalifikované elektronické časová razítka podle Nařízení eIDAS	25
7.1	Certifikát veřejného klíče TSU	25
7.2	Vyhotovování nekvalifikovaných a kvalifikovaných elektronických časových razítek podle Nařízení eIDAS	25
8.	Odkazy	26

1. Úvod

Tento dokument definuje politiku a plnění bezpečnostních požadavků, které se týkají provozní praxe a postupů řízení poskytování důvěryhodné služby vyhotovování kvalifikovaných elektronických časových razítek (dále jen "časové razítko"). Poskytovatelem této důvěryhodné služby je společnost Disig, a.s., se sídlem Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapsaná v obchodním rejstříku OS BA I, odd. Sa, vložka č. 3794 / B (dále jen "Poskytovatel"), prostřednictvím svého systému autority časového razítka (TSA Disig).

Tato politika může být použita pro veřejnou službu poskytování časových razítek tak i pro použití v uzavřených komunitách.

Tento dokument může být použit nezávislými orgány jako základ pro potvrzení, že Poskytovatel je důvěryhodný pro zhotovování časových razítek.

1.1 Přehled

Tato CP TSA se týká poskytování důvěryhodné služby vyhotovování:

- **kvalifikované elektronické časového razítka**
(Identifikátor politiky - A best practices policy for time-stamp (BTSP) ve smyslu EN 319421 [1]: itu-t (0) identified-organization (4) ETSI (0) time-stamp-policy (2023) policy-identifiers (1) best-practices-ts-policy (1)),

ve smyslu ustanovení Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 3. července 2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93 / ES (dále jen "Nařízení eIDAS") [1] a zohlednění ustanovení aktuálních verzí dokumentů Národního bezpečnostního úřadu "Schéma dohledu kvalifikovaných důvěryhodných služeb definovaná orgánem dohledu [2] a" Certifikační politika pro kořenovou CA a důvěryhodnou službu vyhotovování kvalifikovaných certifikátů, jejíž kvalifikovaný statut udělil Národní bezpečnostní úřad "(OID politiky: 1.3.158.36061701.0.0.0.1.2.2) [3] .

Obecné požadavky na poskytování důvěryhodných služeb, na které se odkazuje i tato CP TSA, jsou popsány v dokumentu "Politika poskytování důvěryhodných služeb" [4].

Požizovány kvalifikované elektronické razítka jsou podepisovány s využitím soukromých klíčů jednotek vyhotovujících časová razítka (dále také "TSU"), jejichž certifikáty mohou být vydány výhradně těmito certifikačními autoritami poskytovatele:

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 4/27

Název	Sériové číslo certifikátu	Vydavatel	DigitalID v SK důvěryhodném seznamu
CA Disig	00F4	KCA NBU SR 3	FX9fXwhpKsZwA6H6UWpNrI1fmFM=
CA Disig QCA	077A	KCA NBU SR 3	9FgiC3T8jAqPjDqlhZcvhFnZHyg=

1.2 Název dokumentu a jeho identifikace

Název:	Politika poskytování důvěryhodné služby vyhotovování kvalifikovaných elektronických časových razítek
Zkratka názvu:	CP TSA Disig QTS*
Verze:	4.1
Schválené dne:	18. 7. 2017
Platnost od:	26. 7. 2017
Této CP TSA je přiřazen identifikátor objektu (OID)	1.3.158.35975946.0.0.1.0.4

* - v textu tohoto dokumentu se většinou používá při odkazu pouze zkrácená forma CP TSA

Popis použitého identifikátoru objektu (OID):

1. - ISO assigned OIDs

1.3. - ISO Identified Organization

1.3.158. - Identifikační číslo subjektu (IČO)

1.3.158.35975946. - Disig

1.3.158.35975946.0.0.1. - CA Disig - vyhotovování kvalifikovaných certifikátů

1.3.158.35975946.0.0.1.0.4 - CP TSA Disig QTS

1.3 Účastníci PKI

V rámci poskytování důvěryhodných služeb vyhotovování kvalifikovaných elektronických časových razítek jsou účastníky infrastruktury veřejného klíče entity uvedené v této části.

Soubor	CP_TSA_Disig	Verze	4.1
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017
		Strana	5/27

1.3.1 Jednotka vyhotovování časových razítek

Jednotka pořizování časových razítek:

- je entita, která poskytuje kvalifikované důvěryhodné služby vyhotovování kvalifikovaných elektronických časových razítek uživatelem (Zákazníci, Spoléhající se strany),
- má celkovou odpovědnost za poskytování kvalifikovaných důvěryhodných služeb specifikovaných v odstavci 1.1,
- je uváděna ve vydaných časových razítek jako vydavatel a její soukromé klíče jsou používány při vyhotovování podpisu těchto časových razítek,
- zaručuje, že všechny aspekty jejích služeb, operací a infrastruktury svázané s časovými razítky vydanými podle této politiky jsou prováděny v souladu s jejími požadavky a ustanoveními a v souladu s pravidly na výkon certifikačních činností Poskytovatele.

TSU Poskytovatele jsou součástí hierarchické PKI:

Certifikační autorita KCA NBÚ SR 3 -> CA Disig resp. CA Disig QCA 3 -> TSU

Poskytovatel může provozovat v rámci podřízenosti pod certifikačními autoritami CA Disig resp. CA Disig QCA 3 několik TSU poskytující důvěryhodné služby vyhotovování časového razítka.

1.3.2 Registrační autorita

Registrační autorita (dále jen "RA") je entita, která jedná, na základě smlouvy, jménem Poskytovatele, přičemž vykonává některé vybrané činnosti při poskytování důvěryhodných služeb Poskytovatele.

RA musí vykonávat svou činnost v souladu se schválenou CP TSA a Pravidly na výkon certifikačních činností (dále také "CPS") v aktuálním znění.

Poskytovatel může zřídit RA následujících typů:

- **Komerční RA** - je určena na zprostředkování vybraných kvalifikovaných důvěryhodných služeb Poskytovatele široké veřejnosti a je provozována třetí stranou, na základě písemné smlouvy s Poskytovatelem.
- **Firemní RA** - je určena na zprostředkování vybraných kvalifikovaných důvěryhodných služeb výhradně pro vlastní potřeby konkrétní právnické osoby resp. pro potřeby ní provozovaných systémů vyžadujících použití KC a je provozována na základě písemné smlouvy s Poskytovatelem, danou konkrétní právnickou osobou.
- **Interní RA** - je provozována Poskytovatelem a je určena k poskytování kvalifikovaných důvěryhodných služeb pro všechny zájemce.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 6/27

Poskytovatel v současné době zřizuje pouze RA působící na území Slovenské republiky, které jsou právním subjektem se sídlem v Slovenské republice.

1.3.3 Zákazník

Zákazníkem se rozumí fyzická osoba resp. právnická osoba, jejíž Poskytovatel poskytuje službu vyhotovení časového razítka a ten na koho se vážou závazky odběratele.

Podmínky, které musí splnit Zákazník, definuje tato CP TSA.

Pokud je Zákazníkem právnická osoba, tato může zahrnovat několik koncových uživatelů nebo jediného koncového uživatele. Některé povinnosti, které se vztahují na tuto právnickou osobu, se zároveň vztahují na těchto koncových uživatelů. V každém případě právnická osoba je plně odpovědná pokud povinnosti dané touto CP TSA nejsou ze strany koncových uživatelů správně splněny, a proto je taková organizace odpovědná za vhodnou informovanost svých koncových uživatelů.

Když je Zákazník zároveň koncovým uživatelem, tak je přímo odpovědný, pokud neplní své povinnosti ve smyslu této CP TSA.

1.3.4 Spoléhající se strana

Spoléhající se stranou je fyzická nebo právnická osoba, která se při svém jednání spoléhá na vyhotovenou časové razítko.

1.3.5 Jiní účastníci

Autorita pro správu řádů (Policy Management Authority - dále jen "PMA") je složka Poskytovatele ustanovena za účelem:

- dohledu na vytváření a aktualizací CP TSA, včetně vyhodnocování změn a plánů na provádění libovolných přijatých změn,
- revize CPS, aby se zaručilo, že praxe Poskytovatele vyhovuje příslušné CP TSA,
- revize výsledků auditů, aby se určilo, zda Poskytovatel zodpovědně dodržuje ustanovení vydaných CPS,
- vydávání doporučení pro Poskytovatele týkajících se nápravných a jiných vhodných opatření,
- řízení a usměrňování činnosti Poskytovatele a registračních autorit (dále jen "RA"),
- □ výkladu ustanovení vydaných CPS a svých pokynů pro Poskytovatele a RA,

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 7/27

- výkonu funkce interního auditora, přičemž touto činností pověří samostatného zaměstnance.

PMA představuje vrcholovou složku, která rozhoduje s konečnou platností ve všech záležitostech a aspektech týkajících se Poskytovatele a jeho činnosti.

1.4 Použitelnost časového razítka



Časové razítko vyhotovena ve smyslu požadavků této CP TSA je použitelná všude, kde je vyžadována časové razítko definovaná v článku 42 Nařízení eIDAS. [1]

1.5 Správa politiky

1.5.1 Organizace odpovědná za správu dokumentu

Tabulka č. 1 obsahuje údaje Poskytovatele, který je odpovědný za přípravu, vytvoření a udržování tohoto dokumentu.

Tabulka č. 1: Kontaktní údaje Disig

Poskytovatel	
společnost:	Disig, a.s.
adresa:	Záhradnícka 151, 821 08 Bratislava 2
IČO:	359 75 946
telefon	
e-mail:	
webové sídlo:	http://www.disig.sk

1.5.2 Kontaktní osoba

Pro účely tvorby politik a pravidel má Poskytovatel vytvořenou autoritu pro správu politik (PMA) (viz bod 1.3.5), která plně odpovídá za jejich obsah, a která je připravena odpovědět na všechny otázky týkající se politik a pravidel Poskytovatele.

Tabulka č. 2 obsahuje kontaktní údaje na složku odpovědnou za provoz TSA.

Tabulka č. 2: Kontaktní údaje TSA

Autorita časového razítka CA Disig	
adresa:	Záhradnícka 151, 821 08 Bratislava 2

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 8/27

e-mail:	
telefon	
fax:	
webové sídlo:	

1.5.3 Osoba rozhodující o souladu CP s certifikační politikou

Osobou, která je odpovědná za rozhodování o souladu postupů Poskytovatele, které jsou uvedeny v této CP, je osoba jmenovaná do role PMA.

1.5.4 Postupy schvalování CP a externí politiky

Ještě před začátkem provozu má mít Poskytovatel schválený svůj CP a CPS a musí splňovat všechny jeho požadavky. Obsah CP a CPS schvaluje osoba jmenovaná do role PMA.

Po schválení ze strany PMA je příslušný dokument publikován v souladu s publikační a oznamovací politikou.

1.6 Definice a zkratky

1.6.1 Definice

Pro potřeby tohoto dokumentu jsou použity následující definice převzaty z Nařízení eIDAS [1] resp. normy ETSI EN 319 401 [5]:

Univerzální koordinovaný čas (Coordinated Universal Time (UTC)): časová škála založená na sekundě podle definice v Recommendation ITU-R TF.460-6, "světový čas";

Elektronická časová razítka: údaje v elektronické podobě, které vážou jiné údaje v elektronické formě s konkrétním časem, čímž tvoří důkaz o existenci těchto dalších údajů v daném čase.

Kvalifikovaná elektronická časová razítka: elektronická časová razítka, která splňuje požadavky stanovené v článku 42 Nařízení eIDAS [1]:

Politika časového razítka (Time-stamp policy): definovaný soubor pravidel který svědčí o použitelnosti časového razítka pro konkrétní skupinu a / nebo třídu aplikací se společnými bezpečnostními požadavky;

Autorita časového razítka (Time-Stamping Authority (TSA)): TSP poskytující služby vyhotovování časového razítka použitím jedné nebo více TSU;

Soubor	CP_TSA_Disig	Verze	4.1
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017
		Strana	9/27

Služba vyhotovování časových razítek (Time-stamping service): důvěryhodná služba vyhotovování časových razítek;

Jednotka pořizování časových razítek (Time-Stamping Unit (TSU)): soustava technických a programových prostředků, která je spravována jako jednotka a má v daném čase aktivní jeden klíč na podepisování časových razítek;

Poskytovatel důvěryhodné služby (Trust Service Provider (TSP)): entita, která poskytuje jednu nebo více důvěryhodných služeb;

Pravidla pro provádění certifikačních činností TSA (TSA practice statement): prohlášení o postupech, které TSA používá při pořizování časových razítek, je to specifický typ prohlášení o postupech důvěryhodné služby, jako je definován v normě ETSI EN 319 401 [3];

Systém TSA (TSA system): sestava IT produktů a komponentů zorganizovaných na podporu poskytování služeb vyhotovování časového razítka;

1.6.2 Zkratky

BIPM	– Mezinárodní úřad vah a měr (Bureau International des Poids et Mesures)
BTSP	– svěřené postupy politiky časových razítek (Best practices Time-Stamp Policy)
CA	– Certifikační autorita, autorita vystavuje certifikáty veřejného klíče (Certification Authority)
GMT	– Greenwichský střední čas, čas greenwichského poledníku (Greenwich Mean Time)
IERS	– Mezinárodní referenční služba zemské rotace (International Earth Rotation and Reference System Service)
IT	– informační technologie (Information Technology)
NBÚ	– Národní bezpečnostní úřad
TAI	– Mezinárodní atomový čas (International Atomic Time)
TSA	– Autorita časového razítka, vydavatel časového razítka (Time-Stamping Authority)
TSU	– Samostatná jednotka vytvářející časové razítka (Time-Stamping Unit)
QSCD	– Kvalifikované zařízení na vyhotovování elektronického podpisu / pečeti (Qualified electronic Signature / Seal Creation Device)

Soubor	CP_TSA_Disig	Verze	4.1
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017
		Strana	10/27

2. Úložiště

Úložiště musí být umístěny tak, aby byly přístupné Zákazníkem a spoléhající se strana a v souladu s celkovými bezpečnostními požadavky.

Funkci úložiště Poskytovatele bude zastávat jeho webové sídlo. Přesná URL adresa je uvedena v kapitole 1. Webové sídlo Poskytovatele je prostřednictvím internetu veřejně přístupné Zákazníkům, spoléhající se strana a veřejnosti vůbec.

Veřejně dostupné informace uvedené na webovém sídle Poskytovatele mají charakter řízeného přístupu.

2.1 Zveřejňování informací o TSA

Poskytovatel musí zveřejňovat, v on-line režimu, úložiště, které je přístupné Zákazníkem a spoléhající se strana, které bude obsahovat alespoň tyto informace:

- aktuální CRL jakož i všechny CRL vydané od počátku činnosti vyhotovování časových razítek,
- vlastní certifikáty jednotlivých TSU Poskytovatele, které patří k jejím veřejným klíčem, jejichž odpovídající soukromý klíč je využíván při podepisování vyhotovovaných časových razítek

Poskytovatel musí zveřejňovat v on-line režimu prostřednictvím svého webového sídla tuto CP TSA jakož i další dokumenty související s poskytováním důvěryhodných služeb ve smyslu této CP.

2.2 Frekvence zveřejňování informací

Seznam zrušených certifikátů (CRL) musí být publikován, jak je specifikováno v bodu 4.9.7 aktuálního CP QTSP QCA. Informace o zrušeném certifikátu TSU musí být dostupné na webovém sídle Poskytovatele (viz kapitola 1), který slouží jako jeho úložiště.

CP TSA a CPS TSA případně jejich revize musí být zveřejněny co nejdříve po jejich schválení a vydání.

Veškeré další informace, které mají být publikovány v úložišti, musí publikovat podle možnosti co nejdříve.

2.3 Kontroly přístupu

Poskytovatel musí chránit libovolnou informaci uloženou v úložišti, která není určena pro veřejné rozšíření. Poskytovatel musí vynaložit maximální úsilí na to, aby

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 11/27

zajistil integritu, důvěrnost a dostupnost dat vyplývajících s poskytovaných důvěryhodných služeb. Rovněž musí provést logické a bezpečnostní opatření, aby zabránil neautorizovanému přístupu k úložišti osobám, které by mohly jakýmkoliv způsobem změnit, poškodit, přidat resp. vymazat data uložená v úložišti.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 12/27

3. Obecná ustanovení

3.1 Obecná ustanovení politiky

Tento dokument navazuje na dokument "Politika poskytování důvěryhodných služeb Disig, a.s." [4], kde jsou popsány obecná pravidla poskytovaných důvěryhodných služeb.

Požadavky této politiky jsou založeny na kryptografii veřejného klíče (PKI), certifikátech veřejného klíče a spolehlivého zdroje přesného času.

Očekává se, že odběratelé a spoléhající se strany budou konzultovat podrobnosti způsobu poskytování TSA služby přímo s poskytovající TSU Poskytovatele.

3.2 Služby související s časovým razítkem

Služby související s časovým razítkem je možné z pohledu naplnění požadavků rozdělit na dvě samostatné služby, kterými jsou:

- Poskytování časového razítka - tato služba vytváří samotnou časové razítko.
- Management časového razítka - tato služba monitoruje a řídí procesy vyhotovování časového razítka, aby se zajistilo, že služba je poskytována v souladu s touto CP TSA. Součástí tohoto managementu je proces aktivace resp. de-aktivace služby vyhotovování časového razítka. Management časového razítka například mimo jiné zajišťuje, aby čas použitý

3.3 Vydavatel časových razítek

Poskytovatel důvěryhodné služby vyhotovování časového razítka pro potřeby Zákazníky ve smyslu této CP TSA je společnost Disig.

Poskytovatel musí nést celkovou odpovědnost za poskytování služeb souvisejících s časovým razítkem, jak jsou definovány v odstavci 3.3.

Odpovědnost Poskytovatele za vyhotovování časových razítek je identifikovatelná (viz bod 6.7.1 d))

Poskytovatel může provozovat několik identifikovatelných nezávislých jednotek na vyhotovování časového razítka (TSU).

3.4 Uživatel časového razítka

Uživatelům časového razítka je Zákazník.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 13/27

4. Úvod do politiky časového razítka a plnění obecných požadavků

4.1 Obecně

Tento dokument definuje politiku časového razítka Poskytovatele, která pořizuje časová razítka podporované certifikáty veřejného klíče s přesností lišící se od UTC maximálně o 1000 ms.

4.2 Cíloví uživatelé a použití

4.2.1 Správné praxe uplatňování politiky vyhotovování časových razítek

Tato politika může být použita pro veřejnou službu poskytování časových razítek tak i pro použití v uzavřených komunitách.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 14/27

5. Politiky a pravidla

5.1 Ohodnocení rizik

Viz kapitola 5 dokumentu [4].

5.2 Pravidla pro praktický výkon důvěryhodných služeb

Obecná pravidla pro praktický výkon důvěryhodných služeb jsou uvedeny v [4].

5.3 Všeobecné podmínky

Platí obecné podmínky popsané v dokumentu [4] odstavec 6.2.

5.4 Politika informační bezpečnosti

Politika informační bezpečnosti je popsána v dokumentu [4] odstavec 6.3. [4]

5.5 Závazky Poskytovatele

5.5.1 Obecně

Poskytovatel časového razítka se zavazuje:

- realizovat všechny požadavky kladené na Poskytovatele ve smyslu kapitoly 6 a 7;
- používat bezpečné systémy a zajišťovat dostatečnou bezpečnost postupů, které tyto systémy podporují včetně dostatečné kryptografické bezpečnosti těchto systémů;
- používat bezpečné systémy pro uchovávání časových razítek;
- zajistit, aby praxe vyhotovování časového razítka odpovídala procedurám popsaným v této CP TSA a v souladu s CPS TSA.

5.5.2 Závazky Poskytovatele k Zákazníkovi

Poskytovatel si plní své závazky v souladu s podmínkami poskytování služby časového razítka tak, aby tato služba byla maximálně dostupná a byla prováděna neprodleně a s co největší precizností.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 15/27

5.6 Informace pro spoléhající se strany

Všeobecné podmínky dostupné pro spoléhající se strany (viz odstavec 5.3) musí zahrnovat, v případě, že se spoléhají na časové razítko, následující:

- a) Povinnost ověření, že časové razítko byla správně podepsána a že soukromý klíč použitý k podpisu časového razítka nebyl do doby ověřování kompromitován. Během platnosti certifikátu vydávající TSU musí být platnost jeho podpisového klíče ověřena na základě aktuálního stavu jeho platnosti na základě údajů publikovaných Poskytovatelem.
- b) Všechna omezení pro použití časového razítka podle této politiky.
- c) Všechny další omezení uvedená v dohodách nebo kdekoli jinde.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 16/27

6. Management a provoz TSA Poskytovatele

6.1 Úvod

Management a provoz TSA Poskytovatele jsou prováděna tak, aby přijatá bezpečnostní opatření a nástroje ke kontrole jejich plnění poskytli nezbytnou důvěru, že budou naplněny.

Poskytování časového razítka jako odpověď na požadavek je na rozhodnutí Poskytovatele a závisí na dohodě o úrovni poskytovaných služeb se Zákazníkem.

6.2 Vnitřní organizace

Pro vnitřní organizaci platí ustanovení uvedené v dokumentu [4] odstavec 7.1 a dále tyto:

Poskytovatel:

- a) je právnická osoba podléhající legislativě Slovenské republiky,
- b) má zavedený systém řízení kvality a informační bezpečnosti přiměřený pro poskytované služby vyhotovování časových razítek,
- c) zaměstnává dostatečný počet osob, které mají nezbytné vzdělání, školení, technické znalosti a zkušenosti vzhledem k typu, rozsah a množství práce nezbytné pro poskytování služeb vyhotovování časového razítka.

6.3 Personální bezpečnost

Pro personální bezpečnost platí ustanovení uvedené v dokumentu [4] odstavec 7.2.

6.4 Správa aktiv

Pro správu aktiv platí ustanovení uvedené v dokumentu [4] odstavec 7.3.

6.5 Řízení přístupu

Pro řízení přístupu platí ustanovení uvedené v dokumentu [4] odstavec 7.4.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 17/27

6.6 Kryptografické opatření

6.6.1 Obecně

Vhodné bezpečnostní opatření aplikovány na management jakýchkoliv kryptografických klíčů a kryptografických zařízení během jejich životnosti jsou popsány v dokumentu [4] odstavec 7.5.

6.6.2 Generování klíčů pro TSU

Generování klíčů pro jednotlivé TSU splňuje následující:

- a) a) je provedeno ve fyzicky bezpečném prostředí (viz odstavec 7.8) osobami zařazenými v důvěryhodných rolích (viz odstavec 7.3) za účasti minimálně dvou oprávněných osob. Okruh osob autorizovaných vykonávat tuto funkci je omezen pouze na osoby v rolích vyjmenované v dokumentu CPS TSA.
- b) Generování TSU podpisového klíče (ů) je prováděno v bezpečném kryptografickém zařízení, které je důvěryhodný systém, který splňuje úroveň EAL 4+ resp. FIPS-140-3.
- c) Algoritmus vytváření TSU klíče, výsledná délka klíče a podpisový algoritmus použitý na podepisování časových razítek je v souladu s požadavky normy ETSI TS 119 312 [6]
- d) Podpisový klíč TSU nelze importovat do jiného kryptografického modulu bez rozhodnutí PMA a za účasti stanoveného počtu oprávněných osob.
- e) V kryptografických modulech jednotlivých TSU jsou různé podpisové šifrovací klíče.
- f) TSU má v daném čase k dispozici pouze jeden aktivní klíč na podepisování časového razítka.

6.6.3 Ochrana soukromého klíče TSU

Soukromé klíče TSU zůstávají důvěrné a jejich integrita je udržována minimálně s následujícími požadavky:

- a) Soukromý podpisový klíč TSU je uložen a používán v kryptografickém modulu, který je důvěryhodný systém zabezpečený na úrovni EAL 4+ ve smyslu normy ISO / IEC 15408 [7] resp. splňuje požadavky FIPS 140-3.
- b) Soukromé klíče TSU jsou zálohovány, kopírovány, ukládány a obnovovány jen personálem v důvěryhodných rolích, za dodržení podmínky stanoveného počtu oprávněných osob a ve fyzicky bezpečném prostředí. Autorizované osoby k provádění těchto činností jsou pouze ty, které podléhají pravidlům, které jsou uvedeny v dokumentu [8].

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 18/27

- c) Jakékoliv záložní kopie soukromých podpisových klíčů nacházející se mimo TSU jsou chráněny, tak že je zajištěna jejich integrita a důvěrnost.

6.6.4 Certifikát veřejného klíče TSU

Poskytovatel zaručuje integritu a autenticitu veřejného klíče TSU pro ověření podpisu následovně:

- Veřejný klíč TSU, který slouží k ověření podpisu je dostupný spoléhajícím stranám v certifikátu veřejného klíče.
- Certifikát veřejného klíče TSU pro ověření podpisu je vydán certifikační autoritou poskytující služby ve smyslu normy ETSI EN 319 411-1. [9]
- TSU nevypracuje časové razítko před tím, než jí certifikát veřejného klíče pro ověření podpisu je načten v kryptografickém zařízení TSU.

Když Poskytovatel převezme certifikát veřejného klíče, který slouží k ověření podpisu pro jednotlivé TSU, ověří, že tento certifikát byl správně podepsán, včetně ověření celé certifikační cesty k důvěryhodné certifikační autoritě.

6.6.5 Přepsání klíče TSU

Životnost certifikátu TSU není delší než doba, po kterou je zvolený algoritmus a délka klíče uznány jako vhodné pro tento účel (viz bod 7.6.1c).

6.6.6 Management životního cyklu podpisového kryptografického hardwaru

Aplikované jsou následující požadavky:

- Do kryptografického hardwaru, určeného k podepisování časových razítek, nesmí být svévolně zasahováno během jeho přepravy.
- Do kryptografického hardwaru, který podepisuje časová razítka, nesmí být svévolně zasahováno během jeho skladování.
- Instalace, aktivace a duplikace podpisových klíčů TSU v kryptografickém hardware je prováděna pouze osobami v důvěryhodných rolích, s minimálně dvojitou kontrolou a ve fyzicky bezpečném prostředí (viz odstavec 7.8).
- Soukromé podpisové klíče TSU uložené v kryptografickém modulu TSU jsou v případě vyřazení modulu vymazány takovým způsobem, že je prakticky nemožné jejich obnovení.

6.6.7 Ukončení životního cyklu klíče TSU

Poskytovatel musí definovat datum expirace klíčů TSU.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 19/27

Toto datum nesmí být pozdější než konec platnosti přidruženého certifikátu veřejného klíče, kde musí zohledňovat životnost definovanou v "doporučených velikostech klíče vzhledem k času" z normy ETSI TS 119 312. [6]

Z důvodu schopnosti verifikovat během vhodného intervalu času platnosti časových razítek, může být platnost podpisového klíče TSU redukována.

Datum expirace klíčů TSU může být definován během inicializace kryptografického modulu nebo nastavením periody použití soukromého klíče v certifikátu veřejného klíče TSU.

Soukromý podpisový klíč TSU nebude použit po skončení jeho životního cyklu.

TSA Disig zajistí především, že:

- a) budou použity provozní nebo technické postupy, které zajistí, aby byl použit nový klíč, když klíč TSU vyprší,
- b) soukromé podpisové klíče TSU nebo libovolná část klíče, včetně jakékoliv kopie, budou likvidovány tak, aby soukromé klíče prakticky nebylo možné obnovit.

6.7 Provedení časového razítka

6.7.1 Vydání časového razítka

Časová razítka se musí shodovat s profilem časového razítka podle definice v normě ETSI EN 319 422. [10]

Časová razítka musí být pořizovány bezpečně a musí obsahovat správný čas.

Především:

- a) Hodnoty času, které TSU používá v časové razítku, musí být sledovatelné k alespoň jedné z hodnot reálného času distribuovaného laboratoří UTC (k).
- b) Čas zahrnut do časového razítka musí být synchronizovaný s UTC s přesností definovanou v této politice.
- c) Pokud se zjistí, že hodiny poskytovatele časových razítek (viz bod 7.7.1. b)), potom časová razítka nesmí být vyhotoveny.
- d) Časové razítko musí být podepisována s využitím soukromého klíče vytvořeného pouze pro tento účel.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 20/27

- e) Systém činící časové razítka musí zamítnout jakýkoliv pokus o provedení časového razítka, pokud podpisový soukromý klíč některé TSU Poskytovatele expirují.

6.7.2 Synchronizace hodin s UTC

Čas používaný jednotlivými TSU musí být synchronizovaný s UTC s deklarovanou přesností minimálně s následujícími požadavky:

- a) Kalibrace systémových hodin TSU musí být udržována tak, aby se hodiny neodchýlily od deklarované přesnosti.
- b) Deklarovaná přesnost je 1000 ms nebo lepší.
- c) Hodiny TSU musí být chráněny proti hrozbám, které by mohly způsobit nedetekovatelnou změnu hodin tak, že přesáhnou kalibraci.
- d) Poskytovatel musí ověřovat, zda čas zahrnutý do časového razítka je posunut nebo odchýlen od synchronizace s UTC.
- e) Pokud se zjistí, že čas zahrnut v časové razítka je posunut nebo odchýlen od synchronizace s UTC, TSU musí zastavit vyhotovování časového razítka.
- f) Synchronizace hodin musí být udržována, když nastane přestupná sekunda, kterou oznámila příslušná autorita. Změna zohledňující prostup sekundu nastane během poslední minuty dne, kdy je přestupná sekunda naplánována. Když nastane tato změna, musí být vytvořen záznam o přesném čase, kdy tato změna nastala.

6.8 Fyzická a objektová bezpečnost

Pro fyzickou a objektová bezpečnost platí ustanovení uvedené v dokumentu [4] odstavec 8.6 a dále tyto:

- a) Na kryptografický modul musí být aplikovány řízení přístupu v souladu s odstavcem 6.5.
- b) Na zprávu vyhotovování časových razítek musí být aplikovány následující dodatečná opatření:
- Technické prostředky pro zhotovování časových razítek musí být provozovány v prostředí, které fyzicky a logicky chrání služby před kompromitací, která může být způsobena neautorizovaným přístupem k systémům nebo datům.
 - Každý vstup do fyzicky bezpečné oblasti musí podléhat nezávislému dohledu a neautorizovaná osoba musí být doprovázena autorizovanou

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 21/27

- osobou, pokud je v bezpečné oblasti. Každý vstup a přítomnost musí být zaznamenána.
- Fyzická ochrana musí být dosažena vytvořením jasně definované bezpečnostní hranice (perimetrem, fyzickou bariérou) kolem správy vyhotovování časového razítka. Jakékoliv části objektu sdíleny s jinými organizacemi musí být mimo tento perimetru.
 - Fyzické a objektové bezpečnostní opatření musí chránit objekty, kde jsou umístěny systémy, samotné systémové zdroje a objekty použité na podporu jejich provozu. Bezpečnostní opatření týkající se fyzické a objektové bezpečnosti Poskytovatele musí pokrývat minimálně fyzické řízení přístupu, ochranu před přírodními katastrofami, ochranu před požárem, výpadek podpůrných rozvodů (např. Elektřina, telekomunikace), zhroucení struktury, úniky z potrubí, ochranu proti odcizení, vloupání, a obnovu po pohromě.
 - Přijatá opatření musí chránit zařízení, informace, média a software pro služby vyhotovování časových razítek před vynesemím bez autorizace.

6.9 Provozní bezpečnost

Pro provozní bezpečnost platí ustanovení uvedené v dokumentu [4] odstavec 8.7 a dále toto:

- a) Poskytovatel musí monitorovat kapacitní možnosti poskytované služby a včas projektované do budoucích požadavků na kapacitu, aby se zajistil dostupný adekvátní výkon a úložný prostor.

6.10 Síťová bezpečnost

Pro síťovou bezpečnost platí pro Poskytovatele ustanovení uvedené v dokumentu [4] odstavec 8.8 a dále tyto:

- a) musí udržovat a chránit všechny TSU v bezpečné zóně,
- b) všechny systémy TSU musí být nakonfigurovány tak, že budou mít odstraněny a / nebo zakázané všechny účty, aplikace, služby, protokoly a porty, které nejsou používány pro jejich provoz,
- c) do bezpečných zón a vysoce bezpečných zón mohou mít přístup pouze důvěryhodné role.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 22/27

6.11 Řízení bezpečnostních incidentů

Pro řízení bezpečnostních incidentů platí ustanovení uvedené v dokumentu [4] odstavec 8.9.

6.12 Sběr důkazů

Pro sběr důkazů platí ustanovení uvedené v dokumentu [4] odstavec 8.10 a dále musí být zaznamenávány všechny události týkající se:

- a) řízení životního cyklu klíčů TSU;
- b) řízení životního cyklu certifikátů TSU;
- c) synchronizace hodin TSU s UTC. Toto musí zahrnovat informace týkající se běžné re-kalibrace nebo synchronizace hodin použitých při pořizování časových razítek;
- d) zjištěné ztráty synchronizace.

6.13 Řízení kontinuity činnosti organizace

Pro řízení kontinuity činnosti organizace platí ustanovení uvedené v dokumentu [4] odstavec 8.11 a dále platí: [4] odstavec 8.11 a dále platí:

- a) Plán obnovy po pohromě se musí zabývat kompromitací případně podezřením s kompromitací soukromého klíče TSU nebo ztrátou kalibrace hodin TSU, což mohlo mít vliv na vydané časová razítka.
- b) V případě kompromitace nebo podezření z kompromitace nebo ztrátě kalibrace při pořizování časového razítka musí Poskytovatel zpřístupnit všem odběratelům a spoléhajícím stranám popis kompromitace, která nastala.
- c) V případě kompromitace provozu TSU (např. kompromitace klíče TSU), podezření z kompromitace nebo ztrátě TSU kalibrace nesmí pořizovat časová razítka, pokud nebudou provedeny kroky na obnovu po kompromitaci.
- d) V případě významné kompromitace provozu Poskytovatele nebo ztrátě kalibrace, musí Poskytovatel zpřístupnit všem odběratelům a spoléhajícím stranám informaci, která může být použita pro identifikaci časových razítek, které mohly být ovlivněny, pokud tím neporuší soukromí uživatelů Poskytovatele nebo bezpečnost služeb Poskytovatele.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 23/27

6.14 Ukončení činnosti Poskytovatele a plány ukončení činnosti

Pro ukončení činnosti Poskytovatele platí ustanovení uvedené v dokumentu 8.12 a dále toto:

- a) V případě ukončení služeb Poskytovatele musí být zrušeny všechny certifikáty vydané pro jednotlivé TSU.

6.15 Shoda

Pro shodu platí ustanovení uvedené v dokumentu [4] odstavec 8.13.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 24/27

7. Plnění požadavků pro kvalifikované elektronické časová razítka podle Nařízení eIDAS

7.1 Certifikát veřejného klíče TSU

V smyslu Nařízení eIDAS [1], pro kvalifikované elektronické časová razítka musí být certifikát veřejného klíče TSU, který slouží k ověření podpisu kvalifikované elektronické časového razítka, vydaný certifikační autoritou provozovanou ve smyslu politiky, která vychází z normy ETSI EN 319 411-2 [11].

7.2 Vyhotovování nekvalifikovaných a kvalifikovaných elektronických časových razítek podle Nařízení eIDAS

Pokud TSU zahrnuta v systému Poskytovatele vyhotovuje časová razítka, které jsou vyhlášována jako kvalifikované elektronické razítka podle Nařízení eIDAS [1], tato TSU nesmí pořizovat nekvalifikované elektronické časová razítka.

V případě pořizování nekvalifikovaných elektronických časových razítek musí Poskytovatel používat různé jinou TSU s rozdílným názvem subjektu certifikátu veřejného klíče. Služba takové TSU musí být přístupná přes jiný samostatný přístupový bod.







Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 25/27

8. Odkazy

1. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronicke transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES .
2. Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu. miesto neznámé : Národný bezpečnostný úrad, 3.3.2017. verzia 1.3.
3. Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad. miesto neznámé : Národný bezpečnostný úrad.
4. *Politika poskytovania dôveryhodných služieb Disig, a.s.*
5. *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.* ETSI EN 319 401.
6. *Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.* ETSI TS 119 312.
7. *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.* ISO/IEC 15408-1:2009.
8. *Pravidlá na praktický výkon dôveryhodnej služby časovej pečiatky.* CPS TSA CA Disig.
9. *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.*
10. *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.* ETSI EN 319 422.
11. ETSI EN 319411-2 " *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.*
12. ETSI EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.* ETSI EN 319 421.
13. *RECOMMENDATION ITU-R TF.460-6 Standard-frequency and time-signal emissions.* ITU-R TF.460-6 .
14. RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“.

Soubor	CP_TSA_Disig	Verze	4.1	
Typ	POLITIKA (OID:1.3.158.35975946.0.0.1.0.4)	Datum	26. 7. 2017	Strana 26/27

Historie změn

Verze	Datum	Popis revize; revidoval
1.0	26.2.0007	Prvá verze dokumentu; 
1.1	16. 7. 2007	Změna názvu certifikační autority; 
1.2	28. 1. 2009	Úprava CP v souvislosti s nabytím účinnosti zákona č. 214/2008 Z. Z., kterým se novelizuje zákon č. 215/2002 Z. z. o elektronickém podpisu; 
2.0	23. 12. 2009	Změny v souvislosti se změnou podpisového algoritmu vydávaných časových razítek a změnou profilu TSA certifikátu; 
2.1	31. 3. 2015	Změna OID politiky a stanovení způsobu žádání o poskytnutí akreditované služby časového razítka s OID v žádosti (4.2; 5.2); 
4.1	18. 7. 2017	Komplexní revize v souvislosti s nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) č. 910/2014; 

Disig, a.s.

**Specifikace poskytování důvěryhodné služby vyhotovování kvalifikovaných
elektronických časových razítek**

Obsah

1.	Úvod	3
2.	Odkazy	3
3.	Definice a zkratky	4
3.1	Definice	4
3.2	Zkratky	4
4.	Požadavky na klientské aplikace	5
4.1	Požadavky na klientské aplikace	5
4.1.1	Používané hašovací algoritmy	5
4.2	Profil formátu odpovědi	5
4.2.1	Základní požadavek	5
4.2.2	Podporované algoritmy	5
4.2.3	Délka klíčů	5
5.	Servery časového razítka	5
5.1	Profil žádosti	6
5.2	Provedení časového razítka	6
5.3	Rozhraní pro poskytované TSA služby	7
5.4	Způsob autentizace	7
6.	Demo implementace klientské aplikace	7

1. Úvod

Tento dokument specifikuje službu vyhotovování kvalifikovaných elektronických časových razítek (dále jen "časová razítka"), která je poskytována společností Disig, a.s., se sídlem Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapsaná v obchodním rejstříku OS BA I, odd. Sa, vložka č. 3794 / B (dále jen "Poskytovatel"), prostřednictvím svého systému autority časového razítka (TSA Disig).

Pod službou vyhotovování kvalifikovaných elektronických časových razítek se rozumí poskytování časových razítek v souladu s ustanoveními Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 3. července 2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93 / ES (dále jen "Nařízení eIDAS") [1].

Časová razítka jsou pořizování ve smyslu politiky, která je popsána v dokumentu "Politika poskytování důvěryhodné služby vyhotovování kvalifikovaných elektronických časových razítek", který je k dispozici na webovém sídle poskytovatele <http://eidas.disig.sk/pdf/cp-tsacadisg.pdf>.

Kontaktní osoba odpovědná za poskytování služby časového razítka:

Autorita časového razítka CA Disig (TSA Disig)

adresa: Záhradnícka 151, 821 08 Bratislava 2

e-mail:



telefon

webové sídlo: <http://eidas.disig.sk>

2. Odkazy

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93 / ES.

[2] RFC 3161 Internet X.509 Public Key Infrastructure; Time-Stamp Protocol (TSP); August 2001.

[3] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[4] ETSI EN 319 422 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI);Timestamping protocol and time-stamp token profiles.

3. Definice a zkratky

3.1 Definice

Elektronická časová razítka: údaje v elektronické podobě, které vážou jiné údaje v elektronické formě s konkrétním časem, čímž tvoří důkaz o existenci těchto dalších údajů v daném čase.

Kvalifikovaná elektronická časová razítka: elektronická časová razítka, která splňuje požadavky stanovené v článku 42 Nařízení eIDAS.

Politika časového razítka (Time-stamp policy): definovaný soubor pravidel který svědčí o použitelnosti časového razítka pro konkrétní skupinu a / nebo třídu aplikací se společnými bezpečnostními požadavky;

Autorita časového razítka (Time-Stamping Authority (TSA)): TSP poskytující služby vyhotovování časového razítka použitím jedné nebo více TSU

Služba vyhotovování časových razítek (Time-stamping service): důvěryhodná služba vyhotovování časových razítek

Jednotka pořizování časových razítek (Time-Stamping Unit (TSU)): soustava technických a programových prostředků, která je spravována jako jednotka a má v daném čase aktivní jeden klíč na podepisování časových razítek

System TSA (TSA system): sestava IT produktů a komponentů zorganizovaných na podporu poskytování služeb vyhotovování časového razítka

3.2 Zkratky

TSA – Autorita časového razítka, vydavatel časového razítka (Time-Stamping Authority)

TSU – Samostatná jednotka vytvářející časové razítka (Time-Stamping Unit)

4. Požadavky na klientské aplikace

4.1 Požadavky na klientské aplikace

TSA klient musí podporovat vytvoření žádosti na vyhotovení časového razítka, které je v souladu s požadavky RFC 3161 [3] odstavec 2.4.1 a může podporovat použití těchto polí:

■ reqPolicy

■ nonce

■ certReq

4.1.1 Používané hašovací algoritmy

Klientská aplikace musí akceptovat odpovědi podepsané s použitím algoritmů specifikovaných v ETSI TS 119 312 [3] část A.8.

4.2 Profil formátu odpovědi

4.2.1 Základní požadavek

Klientská aplikace musí podporovat vyhotovenou časové razítka ve formátu, který je definován v RFC 3161 [3] část 2.4.2 a musí podporovat použití pole:

■ Accuracy, a může podporovat použití pole:

■ nonce

4.2.2 Podporované algoritmy

Klientská aplikace musí podporovat minimálně podpisové algoritmy specifikované v ETSI TS 119312 [3] část A.8.

4.2.3 Délka klíčů

Klientská aplikace musí podporovat délku klíčů pro vybrané podpisové algoritmy ve smyslu doporučení ETSI TS 119312 [3] část 9.3.

5. Servery časového razítka

Architektonicky je TSA Disig realizována prostřednictvím několika samostatných TSU (Time-Stamping Unit) jednotek, kde minimálně dvě jsou umístěny v hlavním datovém centru Poskytovatele (primární lokalita) a minimálně dvě jsou umístěny v záložním datovém centru Poskytovatele (záložní lokalita).

Primární lokalita představuje plně redundantní řešení zabezpečené technologickými prostředky k dosažení vysokého výkonu a dostupnosti služby.

Pro dosažení vysoké dostupnosti v případě havarijního stavu primární lokality je zajištěno technickými prostředky přesměrování na záložní lokalitu poskytovatele.

Šifrovací klíče využívané při pořizování podpisu časového razítka jednotlivými TSU TSA Disig jsou uloženy v HSM modulech typu nShield Connect od společnosti THALES, které jsou certifikovány ve smyslu FIPS 140-2 level 3.

TSA Disig poskytuje služby vyhotovování časového razítka na dvou úrovních:

- základní služba (minimální platnost časového razítka 1 rok)
- archivní služba (minimální platnost časového razítka 2 roky)

Po dohodě se zákazníkem může být poskytnuta i jiná úroveň poskytované služby s delší minimální dobou platnosti časového razítka.

5.1 Profil žádosti

Používané servery časového razítka podporují požadavky na provedení časového razítka, které splňují požadavky definované v části 2.4.1 RFC 3161 [3] a podporuje tato pole:

- reqPolicy
- nonce
- certReq

TSA Disig akceptuje jen žádosti obsahující tyto hash informace, pro kterou má být vyhotovena časové razítka:

- sha1
- sha256
- sha512

TSA Disig nepodporuje žádné rozšíření v žádosti o vyhotovení časového razítka.

V případě, že žádost obsahuje pole "nonce" tak i odpověď obsahuje toto pole se stejnou hodnotou.

5.2 Provedení časového razítka

TSA Disig poskytuje časová razítka, které se shodují s profilem časového razítka podle definice v normě ETSI EN 319 422 [2].

TSA Disig poskytuje odpověď na žádost o vyhotovení časového razítka, která splňuje požadavky RFC 3161 [2] část 2.4.2 a obsahuje tato pole:

- policy - v každé odpovědi je uveden OID politiky časového razítka ve tvaru 1.3.158.35975946.0.0.1.0.4

■ genTime - obsahuje hodnotu UTC s odchylkou, která nepřesahuje 500 ms

■ accuracy - obsahuje hodnotu přesnosti, která je stanovena na 500ms

5.3 Rozhraní pro poskytované TSA služby

Služby TSA Disig jsou primárně poskytovány prostřednictvím HTTPS protokolu na těchto adresách:

Základní služba: <https://tsa-aca.disig.sk/tsa>

Archivní služba: <https://tsa-aca.disig.sk/tsa2y>

Po dohodě se zákazníkem je možné ke službě TSA Disig přistupovat i jiným způsobem např. IP port 318, port 80 (http) ap.

5.4 Způsob autentizace

Služba TSA Disig akceptuje primárně pouze žádosti zaslané prostřednictvím HTTPS protokolu (port 443) na adresy uvedené v části Rozhraní pro poskytované TSA služby, kde se musí žádající klientská aplikace autentizovat TS tokenem (softverový X.509 certifikát), který je vydán speciálně pro tento účel poskytovatelem služby.

Po dohodě se zákazníkem může být realizován i jiný způsob autentizace ke službě TSA Disig např. jméno a heslo, případně může být umožněn přístup bez autentifikace z definované IP adresy resp. více IP adres.

6. Demo implementace klientské aplikace

Pro uživatele služby je k dispozici referenční open source implementace klientské aplikace dostupná na adrese:

<https://github.com/disig/TimeStampClient>

PROVÁDĚCÍ SMLOUVA

uzavíraná na základě

Rámcové dohody na zajištění služeb vydávání elektronických časových razítek kvalifikovaným poskytovatelem služeb vytvářejících důvěru 2017-2021

č. j.: xx- xxxxxx/xxxx-2017

Počet listů: 3

1. Smluvní strany:

Název subjektu MV

Sídlo:	Doplní subjekt MV
Její jménem jedná:	Doplní subjekt MV
IČO:	Doplní subjekt MV
DIČ:	Doplní subjekt MV
Bankovní spojení:	Doplní subjekt MV
Číslo účtu:	Doplní subjekt MV

(dále jen „**Objednatel**“)

na straně jedné

a

Disig, a.s.

Sídlo:	Záhradnícka 4871/151, Bratislava, PSČ: 821 08
Její jménem jednájí:	Ing. Ľuboš Batěk, předseda představenstva Ing. Ivan Kühn, místopředseda představenstva
IČO:	35975946
DIČ:	SK2022116976

Bankovní spojení:

Číslo účtu:

BIC (SWIFT):

(dále jen „**Poskytovatel**“)

na straně druhé

(Objednatel a Poskytovatel dále jednotlivě také jako „**Smluvní strana**“ a společně jako „**Smluvní strany**“)

uzavírají níže uvedeného dne, měsíce a roku podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**“) a v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „**zákon o službách vytvářejících důvěru**“), tuto Prováděcí smlouvu o poskytování certifikačních služeb (dále jen „**Smlouva**“). Smlouva je uzavírána na základě „Rámcové dohody na zajištění služeb vydávání elektronických časových razítek

kvalifikovaným poskytovatelem služeb vytvářejících důvěru 2017-2021“ uzavřené dne xx. x. 2017, č.j.: MV-55917-43/VZ-2017 (dále jen „**Rámcová dohoda**“).

2. Předmět Smlouvy

1. Poskytovatel se zavazuje po celou dobu trvání této Smlouvy poskytovat Objednateli následující služby:
 - a) poskytování elektronických časových razítek (dále jen „**TSA**“) v souladu s čl. III. odst. 1 Rámcové dohody.
 - b) vydávání autentizačních certifikátů dle čl. III. odst. 3 Rámcové dohody bude realizováno Poskytovatelem vydáním přístupových tokenů v podobě X.509 certifikátu v softwarové podobě (dále jen „**přístupový token**“).
2. Místa plnění poskytovaných služeb TSA pro Objednatele musí být v souladu s přílohou č. 1 Rámcové dohody.

3. Trvání Smlouvy

1. Tato Smlouva se uzavírá na dobu určitou od 1.. 11. 2017 do 31. 10. 2021 nebo do doby vyčerpání nabídkové ceny uvedené v čl. IX. odst. 6 Rámcové dohody.

4. Cena

1. Cena za vydání jednoho TSA činí **0,06 Kč** bez DPH. K této ceně bude připočtena DPH podle aktuálně platných předpisů dle čl. VIII Rámcové dohody. Cena přístupových tokenů je zahrnuta v cenách za poskytnutí služby TSA a tvoří její nedílnou součást v souladu s ustanovením čl. III odst. 3 Rámcové dohody.
2. Platební podmínky se řídí ustanoveními uvedenými v čl. X Rámcové dohody.
3. Poskytovatel zabezpečí pro Objednatele a Centrálního zadavatele na webovém portále eidas.disig.sk/sk/timestamp/checkts/ zjištění aktuálního stavu poskytovaných služeb TSA pro jednotlivé subjekty MV.

5. Podmínky poskytovaných služeb

1. TSA budou Poskytovatelem vydávána Objednateli v souladu s platnou certifikační politikou pro vydávání kvalifikovaných elektronických časových razítek pouze na základě uzavření této Smlouvy, a to kdykoliv, po dobu trvání Rámcové dohody podle čl. VI. odst. 1 této dohody.
2. Přístupový token služby TSA pro autentizaci včetně návodu na jeho instalaci bude Poskytovatelem vydán a zaslán na e-mailovou adresu kontaktní osoby Objednatele v souladu s platnou certifikační politikou a bude platný po dobu trvání Rámcové dohody.

6. Oprávněné a kontaktní osoby Objednatele

1. Oprávněné osoby Objednatele jsou oprávněny jednat s Poskytovatelem ve věcech poskytování služeb a plnění Smlouvy, které jsou předmětem této Smlouvy a v souladu s Rámcovou dohodou. Subjekty MV jsou zastoupeny oprávněnými osobami Objednatele. Seznam subjektů MV je uveden v příloze č. 1 Rámcové dohody.

2. Seznam kontaktních osob Objednatele je uveden v příloze č. 1 této Smlouvy. Případné změny kontaktních osob je Objednatel povinen do 3 pracovních dnů zaslat Poskytovateli a Centrálnímu zadavateli dle č. IV odst. 3 Rámcové dohody.

7. Závěrečná ustanovení

1. Veškerá ujednání této Smlouvy navazují na Rámcovou dohodu a Rámcovou dohodou se řídí. Povinnosti a vztahy obou Smluvních stran výslovně neupravené touto Smlouvou se řídí příslušnými ustanoveními Rámcové dohody. Smluvní strany se dohodly, že pojmy uvedené v této Smlouvě velkými písmeny mají stejný význam jako tytéž pojmy uvedené v Rámcové dohodě, není-li dále v této Smlouvě stanoveno jinak.
2. Objednatel podpisem této Smlouvy stvrzuje, že je se zněním textu Rámcové dohody seznámen, a s jejím zněním souhlasí.
3. Tato Smlouva nabývá platnosti v den jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění v registru smluv. Smluvní strany berou na vědomí, že tato Smlouva bude uveřejněna v registru smluv dle zákona 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. Dle dohody Smluvních stran zajistí odeslání Smlouvy správci registru smluv Objednatel. Objednatel je oprávněn před odesláním Smlouvy správci registru smluv ve Smlouvě znečitelnit informace, na něž se nevztahuje uveřejňovací povinnost podle zákona o registru smluv.
4. Změny a doplňky této Smlouvy lze provádět pouze písemnými a vzestupně číslovanými dodatky, přičemž každá ze Smluvních stran se zavazuje spravedlivě zvážit návrhy druhé Smluvní strany.
5. Tato Smlouva je vyhotovena podle čl. IX odst. 5 Rámcové dohody minimálně ve třech (3) stejnopisech, z nichž každý bude považován za prvopis.
6. Smluvní strany prohlašují, že Smlouvu uzavírají svobodně a vážně a že obsah Smlouvy vyjadřuje jejich vůli a na důkaz toho Smlouvu podepisují.

Příloha:

Příloha č. 1 – Kontaktní osoby Objednatele

1 strana

Subjekt Ministerstva vnitra

Disig, a.s.

Oprávněná osoba subjektu (doplní subjekt MV)
xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ing. Ľuboš Batěk
předseda představenstva

Ing. Ivan Kühn
místopředseda představenstva

Datum:

Datum:

Číslo prováděcí smlouvy	xxxxxxxxxxxxxx
-------------------------	----------------

Příloha č. 1 Prováděcí smlouvy k Rámcové dohodě na zajištění služeb vydávání elektronických časových razítek kvalifikovaným poskytovatelem služeb vytvářejících důvěru 2017-2021

SEZNAM KONTAKTNÍCH OSOB

Údaje o kontaktních osobách

1.	Jméno		Tituly před	.	Podpis kontaktní osoby
	Příjmení		Tituly za		
	OEČ				
	e-mailová adresa				
	Telefon				

2.	Jméno		Tituly před	.	Podpis kontaktní osoby
	Příjmení		Tituly za		
	OEČ				
	e-mailová adresa				
	Telefon				

3.	Jméno		Tituly před	.	Podpis kontaktní osoby
	Příjmení		Tituly za		
	OEČ				
	e-mailová adresa				
	Telefon				

Legenda:

- 1 Tučně vyznačené položky jsou povinné.
- 2 Osobní evidenční číslo pracovníka subjektu MV (kontaktní osoby).

Kontaktní osoby svým podpisem souhlasí s poskytnutím osobních údajů certifikační autoritě poskytovatele a s jejich zpracováním za účelem prokázání totožnosti v rozsahu jméno, příjmení, OEČ a dále údaje e-mailová adresa a telefon, které slouží pro zasílání informačních zpráv týkajících se poskytovaných kvalifikovaných služeb. Souhlas se uděluje do doby odvolání kontaktní osoby Objednatele, nejdéle však na dobu trvání smluvního vztahu.

Podpisy smluvních stran

za Objednatele

Za Poskytovatele