

SMLOUVA O POSKYTOVÁNÍ SLUŽEB KVALIFIKOVANÁ ELEKTRONICKÁ PEČEŤ A KVALIFIKOVANÉ ELEKTORNICKÉ ČASOVÉ RAZÍTKO

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „Smlouva“)

Smluvní strany

Objednatel:

Obchodní firma	Městská část Praha 9
Se sídlem	Sokolovská 14/324, 180 49 Praha 9
IČ	00063894
DIČ	CZ00063894
Zastoupená	
Bankovní spojení	

(dále jen „Objednatel“)

a

Poskytovatel:

Obchodní firma	ICZ a.s.
Se sídlem	Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
Zapsaná	v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 4840
IČ	25145444
DIČ	CZ699000372
Zastoupená	
Bankovní spojení	

(dále jen „Poskytovatel“)

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



1. PŘEDMĚT SMLOUVY

- 1.1. Předmětem smlouvy je závazek Poskytovatele poskytovat nebo zprostředkovat poskytnutí služby kvalifikovaných elektronických pečeti a časových razítek (dále „**Služby**“) a závazek Objednatele tyto Služby převzít a zaplatit za ně sjednané ceny. Bližší specifikace Služeb je uvedena v Příloze č. 1 Smlouvy.

2. TERMÍN ZAHÁJENÍ POSKYTOVÁNÍ SLUŽEB

- 2.1. Poskytovatel se zavazuje zahájit poskytování Služby (zprovoznit Služby) v prostředí Objednatele nejpozději do 21 dnů od účinnosti této smlouvy za předpokladu poskytnutí nezbytné součinnosti ze strany Objednatele.

3. CENA SLUŽEB A PLATEBNÍ PODMÍNKY

- 3.1. Cena za poskytování Služby se skládá z paušálního poplatku a ceny za 1 ks pečetění s ohledem na množství odebraných elektronických pečeti a časových razítek dle specifikace uvedené v Příloze č. 2 Smlouvy. Dále pak z jednorázové platby za zprovoznění služby také uvedena v Příloze č. 2 Smlouvy.
- 3.2. Ceny uvedené ve Smlouvě jsou uvedeny bez a včetně DPH ve výši platné ke dni uzavření této Smlouvy. Dojde-li ke změně sazby DPH, bude Poskytovatelem DPH účtována podle právních předpisů platných a účinných v době uskutečnění zdanitelného plnění. Takováto změna Smlouvy nemusí být sjednána formou písemného dodatku k této Smlouvě.
- 3.3. Poskytovatel vystaví a zašle Objednateli příslušnou fakturu za poskytnuté Služby vždy bez zbytečného odkladu v měsíci následujícím po skončení příslušného kalendářního měsíce, ve kterém byla poskytována příslušná Služba a to včetně výkazu poskytnutých služeb.
- 3.4. Faktury jsou splatné do patnácti (15) kalendářních dnů od jejich doručení. K uhrazení faktury dojde připsáním částky z účtu Objednatele ve prospěch účtu Poskytovatele.
- 3.5. Jednotlivé faktury musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů, zejména § 29 zák. č. 235/2004 Sb., o dani z přidané hodnoty v platném znění a § 435 zák. č. 89/2012 Sb., občanského zákoníku (dále „**Občanský zákoník**“).

4. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

- 4.1. V rámci realizace předmětu plnění Smlouvy má každá Smluvní strana zejména následující povinnosti:
- i. vzájemně spolupracovat a poskytovat druhé Smluvní straně veškeré informace potřebné pro řádné plnění svých povinností vyplývajících ze Smlouvy;
 - ii. neprodleně informovat druhou Smluvní stranu o vzniku nebo hrozícím vzniku překážky plnění mající významný vliv na řádné a včasné plnění dle Smlouvy;
 - iii. poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle Smlouvy;

- iv. plnit své povinnosti vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním povinností vázaných k jednotlivým termínům a úhradě splatných jednotlivých peněžních dluhů.

5. OCHRANA INFORMACÍ

5.1. Objednatel i Poskytovatel jsou si vědomi toho, že v rámci plnění této Smlouvy:

- i. si mohou vzájemně úmyslně nebo i opomenutím poskytnout informace, které budou považovány za důvěrné, přičemž tyto informace mohou též představovat předmět obchodního tajemství ve smyslu ustanovení § 504 Občanského zákoníku (dále jen „**Důvěrné informace**“);
- ii. mohou jejich zaměstnanci získat vědomou činností druhé Smluvní strany nebo i jejím opominutím přístup k Důvěrným informacím druhé strany.

5.2. Důvěrné informace nezahrnují informace již veřejně známé a informace získané od třetí strany, která byla oprávněna tyto informace šířit.

5.3. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace.

6. OCHRANA OSOBNÍCH ÚDAJŮ

6.1. Smluvní strany nepředpokládají, že v rámci realizace Díla dle této Smlouvy bude docházet ke zpracování osobních údajů Zhotovitelem. V případě, že by v rámci realizace této Smlouvy mělo docházet ke zpracování osobních údajů Zhotovitelem ve smyslu zákona č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů, nebo zákona který jej nahradí, či ve smyslu Nařízení Evropského parlamentu a rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“) od data jeho účinnosti, zavazují se Smluvní strany uzavřít před zahájením zpracování samostatnou smlouvu o zpracování osobních údajů odpovídající zejména požadavkům § 28 odst. 1 a 3 GDPR.

7. OPRÁVNĚNÉ OSOBY SMLUVNÍCH STRAN

7.1. Každá ze Smluvních stran jmenuje oprávněnou osobu. Oprávněné osoby budou zastupovat příslušnou Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy (dále „**Oprávněné osoby**“).

7.2. Oprávněné osoby jsou oprávněny jménem Smluvních stran provádět veškeré úkony v rámci, objednávání Služeb, vyjednávání podmínek a komunikace, akceptačních procedur, zastupovat Smluvní strany ve změnovém řízení a připravovat dodatky ke Smlouvě pro jejich písemné schválení a podpis osobami oprávněnými zavazovat Smluvní strany (statutární orgán), nebo jejich zplnomocněnými zástupci.

7.3. Jména oprávněných osob jako i rozsah jejich oprávnění jsou uvedena v Příloze č. 3 této Smlouvy.

- 7.4. Smluvní strany jsou oprávněny jednostranně změnit Oprávněné osoby bez nutnosti uzavření dodatku ke Smlouvě. V takovém případě jsou povinny na takovou změnu druhou Smluvní stranu předem písemně upozornit, jinak tato změna nemá vůči druhé Smluvní straně právní účinky.

8. TRVÁNÍ SMLOUVY A MOŽNOSTI JEJÍHO UKONČENÍ

- 8.1. Smlouva nabývá platnosti dnem jejího podpisu poslední ze Smluvních stran a uzavírá se na dobu určitou v délce trvání 24 měsíců nebo do vyčerpání finančních prostředků Objednatele ve výši 1 999 999 Kč bez DPH.

- 8.2. Tuto Smlouvu lze ukončit:

- i. Písemnou dohodou Smluvních stran, jejíž součástí je i vypořádání vzájemných závazků.
- ii. Písemným odstoupením od této Smlouvy v případě nepodstatného porušení této Smlouvy druhou Smluvní stranou za podmínek dále stanovených. Jestliže kterákoli Smluvní strana poruší nepodstatným způsobem tuto Smlouvu, je druhá Smluvní strana oprávněna písemně vyzvat porušující Smluvní stranu ke splnění jejích závazků z této Smlouvy. Pokud do třiceti (30) dnů od doručení této výzvy Smluvní strana, která porušila tuto Smlouvu, neučiní uspokojivé kroky k nápravě nebo pokud do šedesáti (60) dnů od této výzvy, nebo do jakékoli delší doby písemně dohodnuté Smluvními stranami, tato Smluvní strana neodstraní porušení závazků této Smlouvy, může druhá Smluvní strana od této Smlouvy odstoupit, aniž by se tím zbavovala výkonu jakýchkoli jiných práv nebo prostředků k dosažení nápravy.

písemnou výpovědí některé ze Smluvních stran, zaslanou druhé Smluvní straně, a to výpovědí bez uvedení důvodu. Výpovědní doba v délce 30 kalendářních dnů počínající běžet prvním dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně

- 8.3. Smluvní strany jsou povinny do třiceti (30) dnů od ukončení účinnosti této Smlouvy vypořádat písemnou dohodou své vzájemné závazky.

9. ZÁVĚREČNÁ USTANOVENÍ

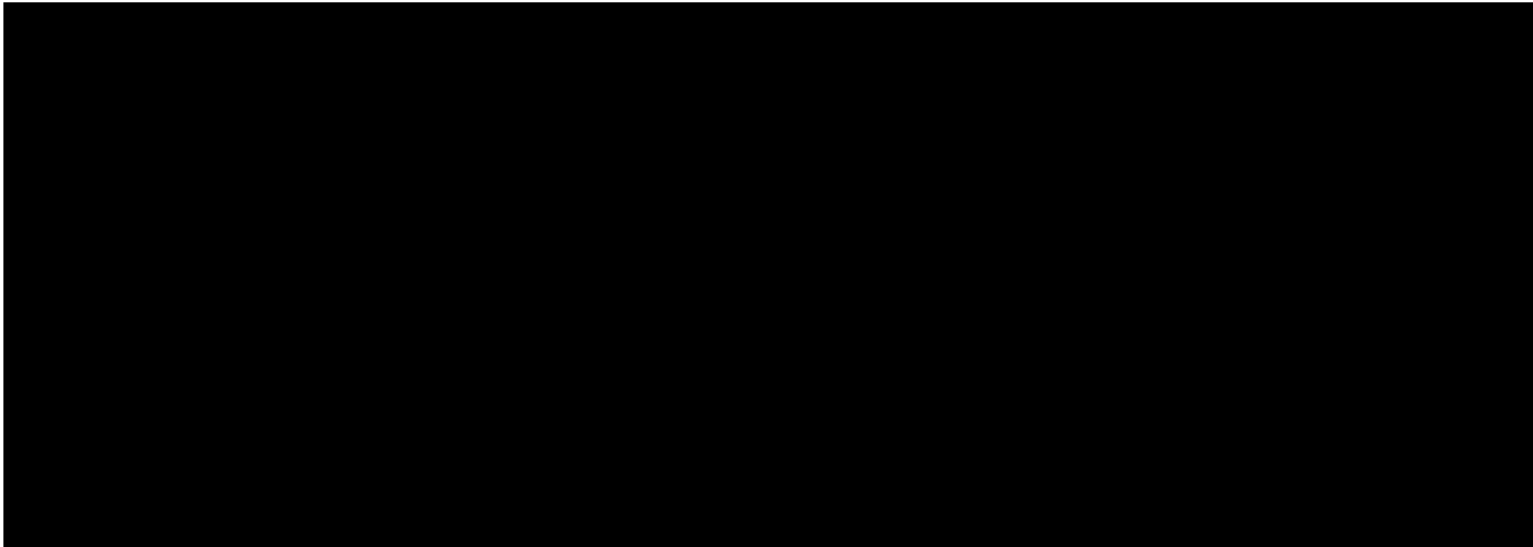
- 9.1. Tato Smlouva nabývá účinnosti ke dni zveřejnění v registru smluv s tím, že Objednatel se zavazuje zveřejnit tuto Smlouvu, jakož i veškeré její případné dodatky v souladu se zákonem o registru smluv.
- 9.2. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti vyplývající z této Smlouvy třetí straně bez předchozího písemného souhlasu druhé Smluvní strany.
- 9.3. Smlouva představuje úplné ujednání mezi Smluvními stranami a nahrazuje všechny dosavadní smlouvy, dohody a ujednání vztahující se k předmětu této Smlouvy, která byla v minulosti učiněna, ať v písemné nebo ústní formě.
- 9.4. Tato Smlouva je vyhotovena ve dvou shodných výtiscích, z nichž Objednatel i Poskytovatel obdrží jedno vyhotovení.
- 9.5. Nedílnou součástí Smlouvy tvoří následující přílohy:

Příloha č. 1 - Specifikace Služeb

Příloha č. 2 – Cena Služeb

Příloha č. 3 - Oprávněné osoby

- 9.6. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.



Příloha č. 1

Specifikace služeb

Služba vytváření kvalifikovaných elektronických pečetí na dálku a kvalifikovaných časových razítek

I.CA RemoteSeal

Východisko služby

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“), konkrétně bod 52 recitálu, články 29 a 39, body 3 a 4 Přílohy II a Příloha III.

Právní základ

Povinnost používat kvalifikované elektronické pečete orgány veřejné moci počínaje 20.9.2018 je dána § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce:

„Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečeti.“

Kvalifikovaná elektronická pečeť dle bodu 27) článku 3 nařízení eIDAS:

„Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.“

Požadavky na kvalifikované prostředky pro vytváření elektronických pečetí (QSealCD):

- prostřednictvím „mutatis mutandis“ stanoveny v Příloze II. nařízení eIDAS
- jedná se o stejné požadavky jako na kvalifikované prostředky pro vytváření elektronických podpisů
- stejné funkční požadavky jako pro SSCD prostředky dle směrnice 1999/93/ES pro ty prostředky, které jsou v držení osoby
- v případě prostředků pro vytváření kvalifikovaných elektronických pečetí na dálku dodatečné požadavky na kvalifikované poskytovatele (odst. 3 a 4 Přílohy II. nařízení eIDAS).

Opečetění dokumentu¶

- Proces opečetění dokumentu inicializuje spisová služba (**obecně volající aplikace**), která má integrovanou knihovnu RSeC. (*podmínka poskytování služby je implementace této knihovny tato smlouva řeší implementaci pouze od ICZ e-spis případně ICZ DESA*)
- Spisová služba předá do RSeC dokument k opečetění spolu s nastavením pečetění (viditelný/neviditelný podpis, formát, přidání TS, atp.) + aktivační soubor vzniklý při aktivaci RSeC
- RSeC připraví dokument k podpisu a sestaví žádost o opečetění (obsahující číslo jednacích dokumentu (obecně jednoznačný textový identifikátor), parametry podpisu, hash původního dokumentu a hash který bude vstupem pro výpočet kryptogramu)
- Tato žádost bude podepsána pomocí **SACi**
- Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS pomocí **SACi**
- Navázaným kanálem předá podepsanou žádost o opečetění na RSeS

- RSeS obratem vrátí do RSeC kryptogramy **CSK_{SACi}** a **CPP**, které budou v RSeC drženy pouze v RAM
- RSeC pomocí **SACi** rozšifruje **CSK_{SACi}** na **SK** a pomocí něj rozšifruje **CPP** na **PP** (vše pouze v RAM, po dešifrování **PP** možno ostatní z RAM uvolnit)
- RSeC následně naváže anonymní HTTPS na DSA s aplikováním certificate pinningu na ověření autenticity DSA
- Následně tímto kanálem po autentizaci pomocí **PP** vytvoří na DSA kryptogram pomocí privátního klíče pečetícího certifikátu
- Po vytvoření kryptogramu se z RAM odstraní **PP**
- RSeC využije kryptogram pro kompletaci podepsaného dokumentu
- Pokud je vyžadován podpis s časovým razítkem, je TS do dokumentu přidáno nyní, přičemž RSeC se vůči TSA autentizuje pomocí **SACi**
- Hotový opečetěný dokument je vrácen spisové službě

Automatické prodloužení služby¶

- Součástí RSeC bude funkcionalita automatické obnovy **SACi** (obdobné řešení jako v QVerify)
- Nejprve se z RSeS stáhne **CSK_{SACi}**
- Pomocí nově vygenerované veřejného klíče se vygeneruje **CSK_{SACj}** a spolu s veřejným klíčem se nahraje na RSeS.
- Následně je možné provést standardní obnovu a nahrát nově vydaný certifikát SACj na RSeS

Obnova pečetícího certifikátu¶

- V rámci automatického prodloužení služby bude také probíhat automatická obnova pečetícího certifikátu
- RSeC s určitým předstihem před vypršením certifikátu vygeneruje na DSA nový pár klíčů a vytvoří žádost o vydání následného certifikátu, kterou opečetí původním certifikátem
- Žádost o následný certifikát se zpracuje na CA standardní cestou
- RSeC následně uloží do DSA následný certifikát a od toho okamžiku jej začne pro pečetení využívat

Podporované formáty podpisu:

- CAdES-B-B, CAdES-B-T
 - Dle normy EN 319 122, ve variantách:
 - Interní
 - Externí
- PAdES-B-B, PAdES-B-T
 - Dle normy EN 319 142, ve variantách:
 - Neviditelný
 - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- XAdES-B a XAdES-T
 - dle normy ETSI TS 103 171, a to ve variantě enveloped, přičemž:
 - Na vstupu bude XML dokument, který bude kompletně použit jakožto vstup podepisovaných data.
 - Na vstupu bude určeno ID elementu, do něž bude jakožto poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť.
 - Na vstupu bude definice požadovaných transformací , digest metody a mime-type referencovaných dat pro element Reference s id="xadesReference".
 - Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512)
 - Na vstupu bude možnost volby podpisu typu XAdES-B/XAdES-T tedy bez nebo s časovým razítkem.

Podpisovaná data (business obsah) nikdy neopouští volající systém (komponentu RSeC)!

Implementace v ICZ e-spis®

Řešení spočívá v implementaci knihovny RemoteSeal Client (RSeC) na serverové straně (server zákazníka, na kterém je instalována komponenta ICZ e-spis® Secure elements), integraci s kvalifikovanou službou pečetění od I.CA s využitím této implementované knihovny a úpravu aplikace ICZ e-spis pro podporu kvalifikované elektronické pečeti.

Při vyslání požadavku na přidání kvalifikované elektronické pečeti Modul eIDAS komunikuje s RSeC, přičemž na vstupu je:

- dokument (hash);
- evidenční číslo (UID komponenty);
- parametry pečeti (typ podpisu, hash algoritmus);
- aktivační e-token;

na výstupu:

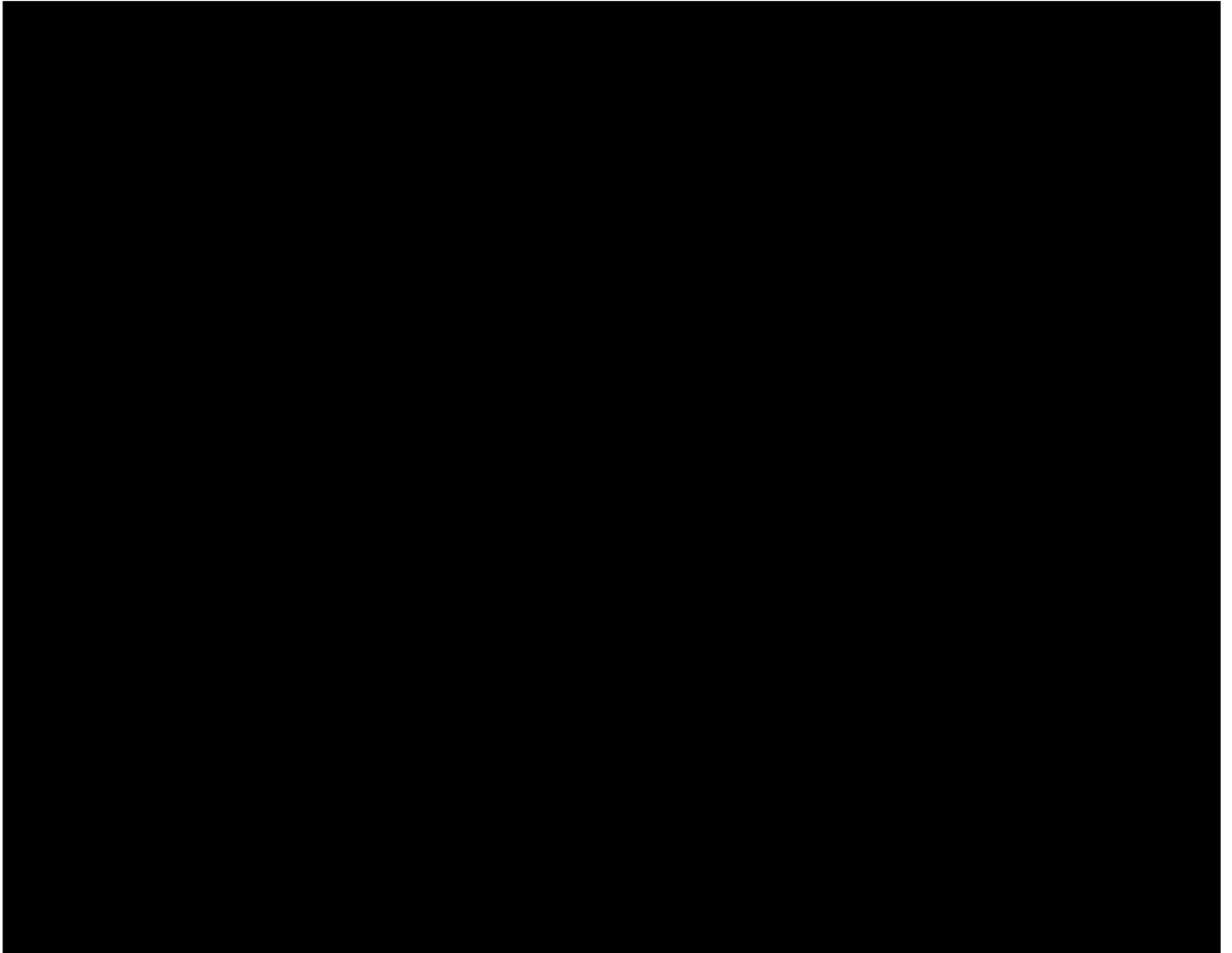
- zapečetěná data pro volající aplikaci ICZ e-spis® – modul eIDAS;
- vytvoření a uložení zapečetěné přílohy(komponenty) k dokumentu dle UID komponenty zaslané na vstupu.

Způsob autentizace ke službě časových razítek

- Autentizace jménem a heslem http;
- Lze využít separátně nejen ke kvalifikované pečeti, ale i ke kvalifikovanému podpisu
- Lze odebírat i v jiných aplikacích kde je třeba opatřit časovým razítkem

Příloha č. 2

Cena Služeb



Příloha č. 3

Oprávněné osoby

