Certifikačná politika

pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok

ver1.1.1

História zmien

Verzia	Dátum vydania	Schválil	Poznámka
1.0	19.2.2021	Richard Margala	Prvá verzia dokumentu.
1.1	27.7.2021	Richard Margala	Zapracovanie opravy gramatických chýb
1.1.1	4.11.2021	Richard Margala	Zapracovanie chýb v terminológii a zlých hyperinkoch

Obsah

1 Úvod

Tento dokument definuje certifikačnú politiku (certification policy, CP) dôveryhodnej služby definovanej v kapitole 3 Účel spoločnosti Ardaco, a.s, so sídlom. Polianky 5, 841 01 Bratislava, zapísanej v Obchodnom registri Okresného súdu Bratislava I, v oddiely Sa, vložka číslo 2903/B.

Základný rámec pre poskytovanie dôveryhodných služieb tvoria:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (nariadenie eIDAS)
- Zákon č. 272/2016 Z.z. z 20. septembra 2016 o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ SR

1.1 Názov dokumentu a jednoznačná identifikácia

Názov dokument a jednoznačná identifikácia	Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania kvalifikovaných elektronických časových pečiatok ver. 1.0
OID	1.3.158.35829036.0.0.0.1.0
ETSI pre časovú pečiatku	BTSP: 0.4.0.2023.1.1 itu- t (0) identified-organization (4) etsi (0) time-stamp-policy (2023) identifikátory politiky (1) best-practices-ts- policy (1)

2 Kontaktné údaje

Adresa sídla spoločnosti	Ardaco, a.s. Polianky 5 841 01 Bratislava Slovenská republika
Internetová adresa	https://tsp.ardaco.com
E-mail:	info@ardaco.com
E-mail pre nahlasovanie incidentov:	incidents@adraco.com

3 Účel

Dôveryhodné služby v zmysle certifikačnej schémy orgánu dohľadu [3] ako aj nariadenia(EÚ) č. 910/2014 [4], ktoré sú organizáciou zabezpečované a popisované v certifikačnej politike:

1. Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok

4 Skratky

CA	Certifikačná autorita
CP	Certifikačná politika
CRL	Zoznam zneplatnených certifikátov (Certification Revocation List)
ČP	Časová pečiatka
PKI	Infraštruktúra verejných kľúčov (Public Key Infrastructure)
RA	Registračná autorita
QSCD	Zariadenie na vyhotovenie kvalifikovanej elektronického podpisu (Qualified Signature Creation Device)

5 Pojmy

koordinovaný svetový čas (UTC) / coordinated Universal Time (UTC) [1]

časová škála založená na druhej, ako je definované v odporúčaní ITU-R TF.460-6
POZNÁMKA: Z praktických dôvodov sa UTC rovná strednému slnečnému času v poludníku (0 °). Presnejšie, UTC je kompromisom medzi vysoko stabilným atómovým časom (Temps Atomique International - TAI) a slnečným časom odvodeným z nepravidelnej rotácie Zeme (v súvislosti s greenwichským stredným siderickým časom (GMST) podľa konvenčného vzťahu) (pozri prílohu C pre viac informácií).

time scale based on the second as defined in Recommendation ITU-R TF.460-6
NOTE: For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship) (see annex C for more details).

spoliehajúca sa strana / relying party [1]

príjemca časovej pečiatky, ktorý sa na túto časovú pečiatku spolieha

recipient of a time-stamp who relies on that time-stamp

predplatiteľ / subscriber [1]

ktorá je viazaná akýmikoľvek povinnosťami predplatiteľa

legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations

časová pečiatka / time-stamp [1]

údaje v elektronickej podobe, ktoré viažu ďalšie elektronické údaje na konkrétny čas, čím sa preukáže, že tieto údaje v tom čase existovali

data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

time-stamp policy [1]
pomenovaný súbor pravidiel, ktorý označuje použiteľnosť časovej pečiatky pre konkrétnu komunitu a / alebo triedu aplikácií so spoločnými bezpečnostnými požiadavkami
POZNÁMKA: Toto je špecifický typ politiky dôveryhodných služieb, ako je definované v ETSI EN 319 401 [2].

named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements
NOTE: This is a specific type of trust service policy as defined in ETSI EN 319 401 [2].

Autorita pre časovú pečiatku / Time-Stamping Authority (TSA) [1]
TSP poskytujúca služby časovej pečiatky pomocou jednej alebo viacerých jednotiek časovej pečiatky

TSP providing time-stamping services using one or more time-stamping units

Služba časovej pečiatky / Time-stamping service [1]
dôveryhodná služba pre vydávanie časových pečiatok

trust service for issuing time-stamps

Jednotka časovej pečiatky / Time-Stamping Unit (TSU) [1]
sada hardvéru a softvéru, ktorá sa spravuje ako jednotka a má súčasne aktívny jeden podpisový kľúč časovej pečiatke

set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time

dôveryhodná služba / trust service [1]
elektronická služba, ktorá zvyšuje dôveru v elektronické transakcie

electronic service that enhances trust and confidence in electronic transactions

Poskytovateľ dôveryhodných služieb / Trust Service Provider (TSP) [1]
subjekt, ktorý poskytuje jednu alebo viac dôveryhodných služieb

entity which provides one or more trust services

TSA system [1]
zloženie IT produktov a komponentov organizované na podporu poskytovania služieb časovej pečiatky

composition of IT products and components organized to support the provision of time-stamping services

UTC [1]
časová škála realizovaná laboratóriom „k“ a udržiavaná v úzkej zhode s UTC s cieľom dosiahnuť ± 100 ns.
POZNÁMKA: Zoznam laboratórií UTC (k) je uvedený v článku 1 obežníka T, ktorý rozširuje BIPM a je k dispozícii na webovej stránke BIPM (http://www.bipm.org/).

time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns. NOTE: A list of UTC(k) laboratories is given in clause 1 of Circular T [i.6] disseminated by BIPM and available from the BIPM website (http://www.bipm.org/).

6 Politiky a postupy (Policies and practices)

6.1 Hodnotenie a posúdenie rizík (Risk assessment)

Uplatňujú sa požiadavky uvedené v ustanovení 5 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

6.2 Vyhlásenie o dôveryhodnej službe (Trust Service Practice Statement)

Uplatňujú sa požiadavky uvedené v ustanovení 6.1 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Vo vyhlásení sú uvedené nasledovné špecifikácie:

a) najmenej jeden algoritmus hash používaný na reprezentáciu časovej pečiatky dátumu;
b) presnosť času v časových pečiatkach vzhľadom na UTC;
c) akékoľvek obmedzenia týkajúce sa používania služby časovej pečiatky;
d) povinnosti predplatiteľa definované v ustanovení 6.5.2, ak existujú;
e) povinnosti spoliehajúcej sa strany definované v ustanovení 6.6;
f) informácie o tom, ako overiť časovú pečiatku tak, aby sa spoliehajúca sa strana považovala za „dôvodne spoliehajúcu sa“ na časovú pečiatku (pozri ustanovenie 6.6) a všetky možné obmedzenia doby platnosti; a
g) akýkoľvek nárok na splnenie požiadaviek na služby časovej pečiatky podľa vnútroštátneho práva.

Taktiež v danom vyhlásení je zahrnutá dostupnosť služby.

6.3 Zmluvné podmienky (Terms and conditions)

Uplatňujú sa požiadavky uvedené v ustanovení 6.2 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

6.4 Politika informačnej bezpečnosti (Information security policy)

Uplatňujú sa požiadavky uvedené v ustanovení 6.3 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

6.5 TSA záväzky (TSA obligations)

6.5.1 Všeobecné podmienky (General)

Organizácia dodržiava všetky povinnosti uvedené v časovej pečiatke, a to buď priamo, alebo začlenené formou odkazu.

6.5.2 Povinnosti TSA voči predplatiteľom (TSA obligations towards subscribers)

Tento dokument neukladá predplatiteľovi žiadne osobitné povinnosti nad rámec akýchkoľvek špecifických požiadaviek organizácie uvedených v podmienkach organizácie.

6.6 Informácie pre spoliehajúce sa strany (Information for relying parties)

Podmienky, ktoré sú k dispozícii spoliehajúcej sa strane (viď kapitola 6.3 Zmluvné podmienky (Terms and conditions)), zahŕňajú povinnosť spoliehajúcej sa strany pred použitím časovej pečiatky:

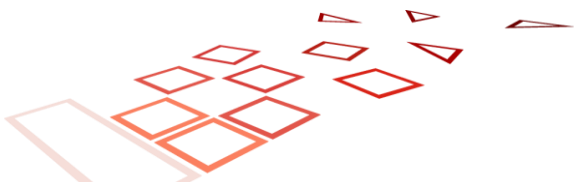
a) overiť, či je časová pečiatka správne podpísaná a či je súkromný kľúč použitý na podpísanie časovej pečiatky;
b) zohľadniť všetky obmedzenia týkajúce sa použitia časovej pečiatky uvedené v politike časovej pečiatky;
c) zohľadniť všetky ďalšie preventívne opatrenia predpísané v dohodách alebo iných naviazaných dokumentoch.

7 Správa a prevádzka TSA (TSA management and operation)

7.1 Úvodné ustanovenia (Introduction)

Účelom nižšie popísaných požiadaviek je jasne definovať požiadavky na naplnenie cieľov organizácie, ku ktorým sa manažment organizácie zaviazal, aby boli napĺňané.

Poskytovanie dôveryhodných služieb a ich dostupnosť je na rozhodnutí organizácie, pričom dohoda medzi organizáciou a spoliehajúcimi sa stranami je na ich vzájomnej dohode.



7.2 Vnútorná organizácia (Internal organization)

Uplatňujú sa požiadavky uvedené v ustanovení 7.1 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Navyše organizácia spĺňa ja tieto osobitné požiadavky:

a) je právnickou osobou podľa vnútroštátneho práva.
b) má systém manažmentu kvality podľa ISO 9000 a implementované požiadavky systému riadenia bezpečnosti informácií vhodné pre služby časovej pečiatky, ktoré poskytuje.
c) zamestnáva dostatočný počet pracovníkov, ktorí majú potrebné vzdelanie, školenie, technické znalosti a skúsenosti týkajúce sa druhu, rozsahu a objemu práce potrebnej na poskytovanie služieb časovej pečiatky. Do zamestnávaného personálu patrí individuálny personál zmluvne zapojený do vykonávania funkcií na podporu služieb časovej pečiatky.

7.3 Personálna bezpečnosť (Personnel security)

Uplatňujú sa požiadavky uvedené v ustanovení 7.2 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.4 Správa majetku (Asset management)

Uplatňujú sa požiadavky uvedené v ustanovení 7.3 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.5 Riadenie prístupov (Access control)

Uplatňujú sa požiadavky uvedené v ustanovení 7.4 normy ETSI EN 319 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.6 Kryptografické kontroly (Cryptographic controls)

7.6.1 Všeobecné podmienky (General)

Uplatňujú sa požiadavky uvedené v ustanovení 7.5 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.6.2 Generovanie kľúča TSU (TSU key generation)

Pre proces generovania kľúča sú uplatňované nasledovné požiadavky:

a) Generovanie podpisového kľúča (-ov) sa uskutočňuje vo fyzicky zabezpečenom prostredí (podľa kapitoly 7.8 Fyzická a environmentálna bezpečnosť (Physical and environmental security)) personálom v dôveryhodných rolách (podľa kapitoly 7.3 Personálna bezpečnosť (Personnel security)) minimálne duálnou kontrolou. Personál oprávnený vykonávať túto funkciu je obmedzený na personál, ktorý má danú funkciu oprávnenie podľa zaradenia.
b) Generovanie podpisového kľúča sa uskutočňuje v bezpečnom kryptografickom zariadení, ktoré:
   i. je definované ako dôveryhodný systém zabezpečený podľa EAL 4
   ii. spĺňa požiadavky uvedené v ISO / IEC 19790 alebo FIPS PUB 140-2, úroveň 3.
   iii. zabezpečené kryptografické zariadenie zodpovedá bodu i).
c) Algoritmus generovania kľúča časovej pečiatku , výsledná dĺžka podpisového kľúča a podpisový algoritmus použitý na podpis kľúča časovej pečiatky je sha256Rsa min 4096 pričom sa riadil špecifikáciou v ETSI TS 119 312
d) Podpisový kľúč sa neimportuje do rôznych kryptografických modulov.
e) Ak sú v rôznych kryptografických moduloch rovnaké kľúče, sú spojené s rovnakým certifikátom verejného kľúča vo všetkých kryptografických moduloch.
f) časová pečiatka musí mať súčasne aktívny jeden podpisový kľúč časovej pečiatky.

7.6.3 Ochrana súkromného kľúča (TSU private key protection)

Organizácia zabezpečuje dôvernosť a integritu súkromných kľúčov dodržiavaním nasledovných pravidiel:

a) súkromný podpisový kľúč je uchovávaný a používaný v kryptografickom module, ktorý:
   i. je dôveryhodný systém, ktorý je zabezpečený na úrovni EAL 4
   ii. spĺňa požiadavky uvedené v ISO / IEC 19790 alebo FIPS PUB 140-2, úroveň 3.
   iii. zabezpečené kryptografické zariadenie by malo zodpovedať bodu i).
b) Nakoľko sú súkromné kľúče zálohované, tak ich kopírovanie, ukladanie a obnovovanie je vykonávané iba pracovníkmi v dôveryhodných rolách, ktorí využívajú aspoň duálne riadenie vo fyzicky zabezpečenom prostredí (pozri odsek 7.8). Personál oprávnený vykonávať túto funkciu je obmedzený len na dôveryhodný personál.
c) Všetky záložné kópie súkromných podpisových kľúčov sú chránené, aby sa zabezpečila ich integrita a dôvernosť kryptografickým modulom pred ich uložením mimo tohto zariadenia.

7.6.4 Certifikát verejného kľúča TSU (TSU public key certificate)

Organizácia zaručuje integritu a autenticitu (verejných) kľúčov na overenie podpisu pričom zaručuje, že:

a) Verejné kľúče na overenie podpisu sú k dispozícii spoliehajúcim sa stranám v osvedčení o verejnom kľúči.
b) Certifikát na overenie podpisu (verejného) je vydávaný certifikačným orgánom pôsobiacim podľa ETSI EN 319 411-1 [3].
c) Organizácia nevydáva časovú pečiatku, kým sa do organizácie alebo do jej kryptografického zariadenia nevloží certifikát na overenie podpisu (verejný kľúč).

Pri získavaní certifikátu na overenie podpisu (verejný kľúč) , organizácia overuje, či bol tento certifikát správne podpísaný (vrátane overenia reťazca certifikátov dôveryhodnej certifikačnej autorite).

7.6.5 Obnova kľúča od TSU (Rekeying TSU's key)

Doba platnosti certifikátu organizácie nesmie byť dlhšia ako časové obdobie, počas ktorého je zvolený algoritmus a dĺžka kľúča uznaná za vhodnú na daný účel (pozri odsek 7.6.2c).

7.6.6 Správa životného cyklu podpisového kryptografického hardvéru (Life cycle management of signing cryptographic hardware)

Organizácia zabezpečuje aj plnenie nasledovných osobitných požiadaviek:

a) Počas prepravy je prísny zákaz manipulácie s kryptografickým hardvérom podpisujúcim časovú pečiatku.
b) Kryptografický hardvér na podpisovanie časovej pečiatky nemá povolenú zmenu kedy a kým je uložený.
c) Inštaláciu, aktiváciu a duplikáciu podpisových kľúčov v kryptografickom hardvéri vykonávajú iba pracovníci v dôveryhodných rolách, ktorí používajú minimálne duálne riadenie vo fyzicky zabezpečenom prostredí (viď kapitola 7.8 Fyzická a environmentálna bezpečnosť (Physical and environmental security)).
d) Kľúče na súkromné podpisovanie uložené v kryptografickom module sa po vyradení zariadenia vymažú takým spôsobom, že je prakticky nemožné ich obnoviť.

7.6.7 Ukončenie životného cyklu kľúča (End of TSU key life cycle)

Organizácia definovala aj dátum vypršania platnosti kľúčov časovej pečiatky. Tento dátum nie je dlhší ako koniec platnosti súvisiaceho certifikátu verejného kľúča. Tento dátum sa berie do úvahy životnosť definovanej v „odporúčaných veľkostiach kľúčov v závislosti od času“ z ETSI TS 119 312 [7].

Dátum vypršania platnosti kľúčov sa určil nastavením obdobia používania súkromného kľúča v rámci certifikátu verejného kľúča. Súkromné podpisové kľúče sa nesmú používať po uplynutí doby ich platnosti.

Životný cyklus kľúčov je ukončený:

1. vypršaním platnosti certifikátu,
2. zrušením platnosti služby TSA v dôveryhodnom zozname a rovnako certifikátu, v prípade mimoriadnej udalosti.

Taktiež sú zabezpečené nasledovné pravidlá:

a) sú zavedené prevádzkové a technické postupy na zabezpečenie zavedenia nového kľúča po uplynutí platnosti kľúča.
b) súkromné podpisové kľúče alebo akákoľvek časť kľúča vrátane akýchkoľvek kópií sa zničí tak, aby nebolo možné získať súkromné kľúče.

7.7 Časová pečiatka (Time-stamping)

7.7.1 Vydanie časovej pečiatky (Time-stamp issuance)

Časové pečiatky zodpovedájú profilu časovej pečiatky vymedzenéj v ETSI EN 319 422 [8]. Časové pečiatky sa vydávajú bezpečne a obsahujú správny čas.

Taktiež sú zabezpečené nasledovné pravidlá:

a) Časové hodnoty, ktoré používa organizácia v časovej pečiatke, sú vysledovateľné aspoň k jednej z hodnôt v reálnom čase distribuovaných laboratóriom UTC (k).
b) Čas zahrnutý v časovej pečiatke sa synchronizuje s UTC s presnosťou stanovenou v politike a, ak je k dispozícii, s presnosťou definovanou v samotnej časovej pečiatke.
c) Ak sa zistí, že hodiny poskytovateľa časovej pečiatky (pozri kapitolu 7.7.2 bod c)) sú mimo stanovenej presnosti (pozri kapitolu 7.7.1 bod b)), časové pečiatky sa nevydávajú.
d) Časová pečiatka sa podpisuje pomocou kľúča vygenerovaného výlučne na tento účel.
e) Systém generovania časových pečiatok odmietne akýkoľvek pokus o vydanie časových pečiatok po dosiahnutí konca platnosti súkromného kľúča organizácie.

7.7.2 Synchronizácia hodín s UTC (Clock synchronization with UTC)

Hodiny organizácie časovej pečiatky sa synchronizujú s UTC, ktorá je hlavným výstupom Státního etalonu frekvence a času Českého metrologického institutu (ČMI). ČMI aplikuje opatrenia, aby časová odchýlka nevybočila z tolerancie UTC − UTC(TP) ± 100 ns. UTC (TP) je šírená prostredníctvom NTP servera na adrese time.ufe.cz. Monitorovanie funkčnosti synchronizácie so systémami na strane TSP a reakcia na stratu synchronizácie je predmetom Plánu riadenia reakcie na incidenty [12] tak, aby odchýlka presnosti časovej pečiatky nevybočila z tolerancie ±1 s.

Taktiež sú zabezpečené nasledovné požiadavky:

a) Kalibrácia hodín sa udržiava tak, aby sa hodiny neodchyľovali mimo deklarovanej presnosti.
b) Deklarovaná presnosť je najmenej ako 1 sekunda.
c) Hodiny sú chránené pred hrozbami
d) Spoliehajúce sa strany sú oboznámene sa s hrozbou v prípade ak sa zistí, že sa čas, ktorý by bol uvedený v časovej pečiatke, posunul alebo zoskočil zo synchronizácie s UTC.
e) Ak sa zistí, že čas, ktorý by bol uvedený v časovej pečiatke, sa posunie alebo vyskočí zo synchronizácie s UTC, organizácia zastaví vydávanie časovej známky.
f) Synchronizácia hodín je zabezpečená.

7.8 Fyzická a environmentálna bezpečnosť (Physical and environmental security)

Uplatňujú sa požiadavky uvedené v ustanovení 7.6 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Navyše platia tieto osobitné požiadavky:

a) Na kryptografický modul uplatňujú kontroly prístupu, aby sa splnili požiadavky bezpečnosti kryptografických modulov uvedené v ustanovení 7.6.
b) Na správu časových pečiatok sa vzťahujú tieto ďalšie kontroly:
    i. Zariadenia na správu časových značiek sa prevádzkujú v prostredí, ktoré fyzicky a logicky chráni služby pred kompromismi prostredníctvom neoprávneného prístupu k systémom alebo údajom.
    ii. Každý vstup do fyzicky zabezpečeného priestoru podlieha nezávislému dohľadu a neautorizovaná osoba musí byť v zabezpečenom priestore sprevádzaná autorizovanou osobou. Každý záznam a existencia sa zaznamená.

iii. Fyzická ochrana sa dosiahne vytvorením jasne definovaných bezpečnostných obvodov (t. j. fyzických bariér) okolo riadenia časových pečiatok. Všetky časti priestorov zdieľané s inými organizáciami musia byť mimo tohto obvodu

iv. Fyzické a environmentálne bezpečnostné kontroly chránia zariadenie, v ktorom sú umiestnené systémové zdroje, samotné systémové zdroje a zariadenia používané na podporu ich prevádzky. Politika organizácie v oblasti fyzickej a environmentálnej bezpečnosti pre systémy zaoberajúce sa riadením časových pečiatok definuje minimálne kontrolu fyzického prístupu, ochranu pred prírodnými katastrofami, faktormi požiarnej bezpečnosti, zlyhaním podporných služieb (napr. energia, telekomunikácie), kolapsom štruktúry, vodovodnými netesnosťami, ochrana proti krádeži, rozbitiu a vniknutiu, a zotavenie po katastrofe.

v. Ovládacie prvky chránia pred vybavením, informáciami, médiami a softvérom súvisiacim so službami časovej pečiatky odobratými mimo server bez oprávnenia. V rovnakej zabezpečenej oblasti sú podporované ďalšie funkcie nakoľko prístup je obmedzený iba na oprávnený personál.

7.9 Bezpečnosť prevádzky (Operational security)

Uplatňujú sa požiadavky uvedené v ustanovení 7.7 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.10 Sieťová bezpečnosť (Network security)

Uplatňujú sa požiadavky uvedené v ustanovení 7.8 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Navyše platia tieto osobitné požiadavky:

a) organizácia udržiava a chráni všetky systémy časovej pečiatky v zabezpečenej zóne.
b) organizácia nakonfiguruje všetky systémy odstránením alebo zakázaním všetkých účtov, aplikácií, služieb, protokolov a portov, ktoré sa nepoužívajú v operáciách.
c) do zabezpečených zón a zón s vysokým zabezpečením majú prístup iba dôveryhodné role.

7.11 Incident management

Uplatňujú sa požiadavky uvedené v ustanovení 7.9 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

7.12 Zhromažďovanie dôkazov (Collection of evidence)

Uplatňujú sa požiadavky uvedené v ustanovení 7.10 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Navyše platia tieto osobitné požiadavky pre záznamy všetkých udalostí:

a) týkajúcich sa životného cyklu kľúčov sú zaznamenané.
b) týkajúcich sa životného cyklu certifikátov (ak je to vhodné) sú zaznamenané.
c) týkajúcich sa synchronizácie hodín s UTC sú zaznamenané do denníka, ktorý obsahuje aj informácie týkajúce sa bežnej rekalibrácie alebo synchronizácie hodín použitých pri časovej pečiatke.
d) súvisiacich s detekciou straty synchronizácie sú zaznamenané.

7.13 Riadenie kontinuity činnosti (Business continuity management)

Uplatňujú sa požiadavky uvedené v ustanovení 7.11 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Ďalej platia tieto osobitné požiadavky:

a) Plán obnovy po katastrofe sa taktiež zameriava na kompromitáciu alebo podozrenie z kompromitácie súkromných podpisových kľúčov TSU alebo stratu kalibrácie hodín TSU, čo môže mať vplyv na vydané časové pečiatky.
b) V prípade kompromitácie alebo podozrenia s kompromitácie alebo straty kalibrácie pri vydávaní časovej pečiatky sa sprístupnia všetkým predplatiteľom a spoliehajúcim sa stranám popis kompromitácie, ku ktorej došlo.
c) V prípade ohrozenia prevádzky (napr. kompromitácia kľúča), podozrenia na kompromitáciu alebo stratu kalibrácie organizácia nebude vydávať časové pečiatky, kým nebudú podniknuté kroky na zotavenie sa z danej situácie.
d) V prípade závažného ohrozenia fungovania alebo straty kalibrácie bude poskytnuté všetkým predplatiteľom a spoliehajúcim sa stranám informácie, ktoré možno použiť na identifikáciu časových pečiatok, ktoré mohli byť ovplyvnené, pokiaľ to neporuší súkromie používateľom alebo bezpečnosťou služieb.

7.14 Ukončenie TSA a plány ukončenia (TSA termination and termination plans)

Uplatňujú sa požiadavky uvedené v ustanovení 7.12 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

Navyše je zabezpečené pri ukončení služby, že organizácia vykoná aj zrušenie certifikátov.

7.15 Súlad (Compliance)

Uplatňujú sa požiadavky uvedené v ustanovení 7.13 normy ETSI EN 319 401 [2], ktoré sú definované v samostatnom dokumente Certifikačná politika pre služby vyhotovovania a overovania kvalifikovaných certifikátov.

8 Ďalšie požiadavky na kvalifikované elektronické časové pečiatky podľa nariadenia (EÚ) č. 910/2014 (Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014)

8.1 Certifikát verejného kľúča TSU (TSU public key certificate)

Ak sa požaduje, aby časová pečiatka bola kvalifikovanou elektronickou časovou pečiatkou podľa nariadenia (EÚ) č. 910/2014, certifikát na overenie podpisu (verejného) vydáva certifikačný orgán pôsobiaci podľa certifikačnej politiky ETSI EN 319 411-2 ako aj požiadavky ETSI EN 319 411-1.

Od spoliehajúcej sa strany sa očakáva, že použije dôveryhodný zoznam na zistenie, či sú jednotka časovej pečiatky a časová pečiatka kvalifikované. Ak je verejný kľúč organizácie uvedený v zozname dôveryhodných služieb a služba, ktorú predstavuje, je kvalifikovanou službou časovej pečiatky, potom sa časové pečiatky nami vydané považujú za kvalifikované. QcStatement "esi4-qtstStatement-1", ako je definované v ETSI EN 319 422, odsek 9.1, sa používa ako indikácia, že organizácia tvrdí, že časová pečiatka je kvalifikovaná elektronická časová pečiatka.

8.2 TSA vydávajúci nekvalifikované a kvalifikované elektronické časové pečiatky podľa nariadenia (EÚ) č. 910/2014 (TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014)

Keďže organizácia vydáva časové pečiatky klasifikované ako kvalifikovaná elektronická časová pečiatka podľa nariadenia (EÚ) č. 910/2014 [5] tak táto časť organizácie (TSU) nevydáva nekvalifikované elektronické časové pečiatky. V takom prípade TSA použije vo svojom certifikáte verejného kľúča rôzne TSU identifikované rôznymi názvami subjektov. Tieto TSU sú prístupné prostredníctvom samostatných prístupových bodov k službám.

Vďaka vyššie spomenutému a nariadeniam, je preto možné mať rôzne TSU s iným hardvérom / softvérom, pre rôzne certifikáty verejného kľúča a samostatné prístupové body k službe.

9 Referencie

[1] ETSI EN 319 421 V1.1.1 (2016-03): Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers issuing Time-Stamps https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

[2] ETSI EN 319 401 V2.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);General Policy Requirements for Trust Service Providers - https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf

[3] ETSI EN 319 411-1 V1.1.1 (2016-02): Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates;Part 1: General requirements - https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[4] https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32014R0910

[6] ISO/IEC 27002:2013 Information Security Management standard - https://www.praxiom.com/iso-27002.htm

[7] ETSI TS 119 312 V1.2.1 (2017-05)Electronic Signatures and Infrastructures (ESI); Cryptographic Suites - https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf

[8] ETSI EN 319 422 V1.1.0 (2015-12)Electronic Signatures and Infrastructures (ESI);Time-stamping protocol and time-stamp token profiles - https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.00_30/en_319422v010100v.pdf

[9] Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu v1.4 - https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/docs/SchemaDohladu.pdf

[10] Zákona 272/2016 Z. z. v znení neskorších predpisov o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

[11] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES - https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32014R0910

[12] Plán riadenia reakcie na incidenty – interný dokument