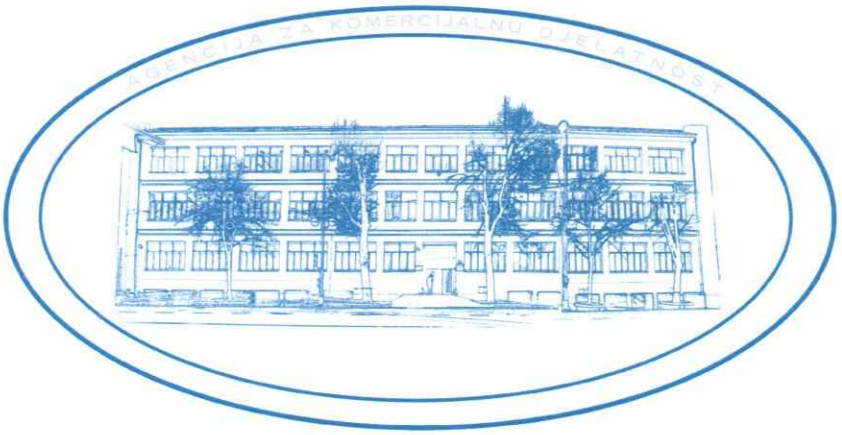

AKD QTSA PRAVILA I POSTUPCI PRUŽANJA USLUGA IZDAVANJA VREMENSKOG ŽIGA

Izdanje 1.0

Status: 14. 02. 2018.

SADRŽAJ

Naziv dokumenta

Oznaka :	PRO-I-94-01
Puni naziv:	AKD QTSA Pravila i postupci izdavanja vremenskog žiga
Skraćeni naziv:	AKD TSP/PS
Izdanje:	1.0/2018-02-14
Effectiv date:	14.02.2018.
OID:	1.3.6.1.4.1.43999.5.7
Tip dokumenta:	Time Stamp Policy, TSA Practice Statement
Dostupnost:	http://id.hr/cps

Povijest promjena dokumenta

Izdanje	Datum	Obrazloženje izmjene
1.0	14.02.2018.	Prvo izdanje dokumenta

Kontakt informacije

AKD kontakt informacije:	AKD d.o.o Savska cesta 31, 10000 Zagreb, Hrvatska Web portal: http://akd.hr e-mail: akd@akd.hr
AKD QTSA kontakt informacije:	AKD d.o.o - PMA Savska cesta 31, 10000 Zagreb, Hrvatska Web portal: http://id.hr/tsa e-mail: pma@akd.hr Služba za korisnike: Helpdesk-kID@akd.hr

Uvod

Agencija za komercijalnu djelatnost, proizvodno, uslužno i trgovačko d.o.o. (u daljnjem tekstu: AKD) je pravna osoba koja djeluje kao kvalificirani pružatelj usluga povjerenja u smislu Uredbe (EU) br. 910/2014 [1].

AKD izdaje elektroničke vremenske žigove, certifikate za elektroničku identifikaciju i certifikate za elektronički potpis. AKD-ova usluga izdavanja elektroničkog vremenskog žiga naziva se AKD QTSA.

Elektronički vremenski žig (dalje u tekstu vremenski žig) kojim se bavi ovaj dokument omogućava naknadnu provjeru elektroničkog potpisa te dokazivanje:

1) da je podatak postojao prije nekog određenog vremena, a svakako u trenutku kada je izrađen elektronički potpis,
2) da je elektronički potpis izrađen u trenutku kada je certifikat korisnika bio valjan i
3) da je elektronički potpis izrađen prije datuma i vremena koji su sadržani u vremenskom žigu.

To je posebno značajno u sljedećim okolnostima:

- prije isteka perioda važenja certifikata kada je došlo je do opoziva certifikata što može ukazivati na postojanje mogućnosti kompromitacije privatnog ključa korisnika te
- nakon isteka perioda važenja certifikata kada elektronički potpis treba i dalje vrijediti, a kada certifikacijsko tijelo (CA) više nije dužno obrađivati informacije o statusu isteklih i nevažećih certifikata.

AKD-ove jedinice za izradu vremenskog žiga (*eng. Time-Stamping Units - TSUs*) izdaju kvalificirane elektroničke vremenske žigove sukladno zahtjevima utvrđenim Uredbom (EU) br. 910/2014 [1].

Javni ključevi AKD TSU jedinica kao i javni ključ certifikacijskog tijela KIDCA koje izdaje certifikate za AKD TSU jedinice, nalaze se na Pouzdanom popisu kojeg u Republici Hrvatskoj vodi središnje tijelo državne uprave nadležno za poslove gospodarstva.

1. Opseg

Ovaj dokument AKD QTSA Pravila i postupci izdavanja vremenskog žiga (u daljnjem tekstu: AKD TSP/PS) specificira sigurnosne zahtjeve te organizacijske i tehničke mjere koje AKD u praksi primjenjuje prilikom pružanja usluga izdavanja vremenskog žiga.

AKD TSP/PS odgovara dokumentima *„Time-stamp Policy"* i *„TSA practice statement"* koji su definirani u normi ETSI EN 319 421 [11], a s kojom su usklađeni struktura i sadržaj ovog dokumenta.

AKD TSP/PS namijenjen je:

- korisnicima i pouzdajućim stranama kojima su potrebne detaljnije informacije o njihovim pravima i obvezama, kao i o pravima i obvezama pružatelja usluga povjerenja,
- pružatelju usluga povjerenja kako bi uredio pravila i postupke pružanja usluga te osigurao provedbu sigurnosnih zahtjeva u praksi,
- tijelima za ocjenjivanje sukladnosti i nadzornim tijelima za procjenu sposobnosti AKD-a za pružanje usluga izdavanja vremenskog žiga i nošenje status kvalificiranog pružatelja usluge.

U sklopu AKD-a djeluje Povjerenstvo za upravljanje pravilima certificiranja *(eng: Policy Management Authority PMA)* koje je odgovorno za održavanje i odobravanje ovog dokumenta kao i svih pravila i postupaka vezanih uz djelovanje AKD PKI. Upravljačke strukture AKD-a odgovorne su za pravilnu implementaciju i provedbu pravila i postupaka koje donosi PMA.

Ovaj dokument treba čitati skupa s AKD PKI Općim pravilima pružanja usluga certificiranja [23] i kIDCA Pravilnikom o postupcima certificiranja [24] (u daljnjem tekstu: AKD CP/CPS).

AKD će informirati javnost o promjenama AKD TSP/PS koje namjerava provesti te će nakon formalnog odobrenja, po postupku definiranom u točki 1.5 AKD CP/CP, izmijenjeni dokument objaviti i učiniti ga dostupnim korisnicima i pouzdajućim stranama

2. Reference

[1] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.

[2] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17).

[3] Zakon o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15)

[4] Zakon o zaštiti potrošača (NN 41/14, 110/15)

[5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[6] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions"

[7] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

[8] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[10] ETSI EN 319 411-2: "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".

[11] ETSI EN 319 421: " Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[12] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[13] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

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

[15] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[16] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[17] CEN TS 419 261:2015: "Security Requirements for Trustworthy Systems Managing certificates and time-stamps ".

[18] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".

[19] ISO/IEC 27001:2013: " Information technology — Security techniques — Information security management systems — Requirements".

[20] ISO/IEC 27002:2013: „Information Technology – Security Techniques – Code of practice for information security controls".

[21] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[22] ISO/IEC 9001:2015: "Quality management systems - Requirements".

[23] CP: AKD PKI Opća pravila pružanja usluga certificiranja

[24] CPS: kIDCA Pravilnik o postupcima certificiranja

3. Definicije i kratice

3.1. Definicije

Opće definicije pojmova koji se koriste u ovome dokumentu navedene su u AKD CP/CPS. Definicije pojmova koje su specifične za ovaj dokument su:

Pravila i postupci izdavanja vremenskog žiga ili **AKD TSP/PS** (*eng. Time-Stamp Policy/ Practice Statement*): Imenovani skup pravila koji ukazuje na prikladnost vremenskog žiga za određenu

skupinu i/ili grupu primjena sa zajedničkim sigurnosnim zahtjevima i postupci koji se primjenjuju kod izdavanja vremenskog žiga.

C ili **AKD TSDS** *(eng. TSA Disclosure statement or TSA Terms and Conditions)*: Imenovani skup pravila i postupaka koje primjenjuje TSA, koja se posebno ističu i objavljuju korisnicima i pouzdajućim stranama, primjerice, kako bi se udovoljilo regulatornim zahtjevima.

Koordinirano svjetsko vrijeme (*eng. Coordinated Universal Time - UTC*): Vremenska ljestvica koja se temelji na sekundi kako je definirano u normi ITU-R TF.460-6 [6]. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (Temps Atomique International – TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvjezdano vrijeme (GMST)).

Pouzdajuća strana (*eng. Relying party):* primatelj vremenskog žiga koji se pouzdaje u taj vremenski žig.

Korisnik (*eng. Subscriber*): Pravna ili fizička osoba kojoj je izdan vremenski žig i koja je dužna poštivati preuzete odgovornosti.

Elektronički vremenski žig ili Vremenski žig: Podaci u elektroničkom obliku koji povezuju druge podatke u elektroničkom obliku s određenim vremenom i na taj način dokazuju da su ti podaci postojali u to vrijeme.

Kvalificirani elektronički vremenski žig Elektronički vremenski žig koji ispunjava sljedeće zahtjeve:

a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka;

b) temelji se na izvoru točnog vremena povezanom s koordiniranim svjetskim vremenom; i

c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.

Usluga izdavanja vremenskog žiga *(eng. Time-stamping service)*: Usluga povjerenja za izdavanje vremenskih žigova.

Pružatelj usluga izdavanja vremenskog žiga (*eng. Time-Stamping Authority - TSA*): Pružatelj usluge izdavanja vremenskog žiga koji koristi jednu ili više jedinica za izradu vremenskog žiga.

Jedinica za izradu vremenskog žiga (*eng. Time-Stamping Unit - TSU*): Skup hardvera i softvera združen u jednu cjelinu koja u danom trenutku ima samo jedan aktivan potpisni ključ za izradu vremenskog žiga.

Token vremenskog žiga *(eng. TimeStampToken - TST)*: Podatkovni objekt definiran u IETF RFC 3161 [15] koji predstavlja vremenski žig.

AKD QTSA sustav (*eng. TSA system*): Skup IT proizvoda i komponenti organiziranih za pružanje usluga izdavanja vremenskog žiga.

UTC(k): Vremenska skala koja se ostvaruje u laboratoriju „k" i koja se čuva u bliskom dogovoru s UTC, a s ciljem postizanja ± 100 ns.

3.2. Kratice

Opće kratice koji se koriste u ovome dokumentu navedene su u AKD CP/CPS.

Ostale kratice specifične za ovaj dokument su:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4. Osnovni koncepti

4.1. Općenito

Koncept pružanja usluga izdavanja vremenskog zasnovan je na općim pravilima za pružatelje usluga povjerenja prema normi ETSI EN 319 401 [7] i specifičnim pravilima za vremenski žig prema normi ETSI EN 319 421 [11].

Vremenski žig koji se izdaje u skladu s ovim AKD TSP/PS je elektronički vremenski žig. Primijenjena tehnologija izdavanja vremenskih žigova zasnovana je na kriptografiji javnog ključa, X 509 certifikatima i na pouzdanom izvoru vremena.

4.2. Usluge izdavanja vremenskog žiga

Usluge izdavanja vremenskog žiga sastoje se od sljedećih komponenata:

a) **Usluga dostave vremenskog žiga** koja obuhvaća tehničke komponente potrebne za generiranje vremenskog žiga odnosno za izdavanje tokena vremenskog žiga (*eng. Time Stamp Token -TST*).

b) **Usluga upravljanja vremenskim žigom** koja obuhvaća komponente usluge koje nadziru i kontroliraju postupke izdavanja vremenskog žiga, uključujući instalaciju i deinstalaciju tehničkih komponenti sustava, sinkronizaciju s referentnim izvorom vremena – UTC i provedbu ostalih postupaka kako je definirano u ovom AKD TSP/PS.

c) **Usluga informiranja** koja obuhvaća AKD QTSA portal, objavljivanje AKD TSP/PS and AKD TSDS te informiranje korisnika i pouzdajućih strana o izdavanju vremenskih žigova i korištenju usluga AKD QTSA.

Kako bi se osigurala kvaliteta i povećala vjerodostojnost usluge izdavanja vremenskog žiga, AKD QTSA postupa sukladno najboljim pravilima struke (*eng. Best practices Time-Stamp Policy - BTSP*) i normama koje su referencirane u točki 2 ovoga dokumenta.

4.3. Pružatelj usluga izdavanja vremenskog žiga - TSA

Pružatelj usluge izdavanja vremenskog žiga (dalje u tekstu TSA) je tijelo uspostavljeno u AKD-u koje pruža usluge izdavanja vremenskog žiga koje su pobrojane u točki 4.2 ovoga dokumenta i koje djeluje u skladu s pravilima i postupcima koji su opisani u ovom AKD TSP/PS.

TSA je odgovoran za rad TSU i izdavanje TST te snosi punu odgovornost za ispunjenje zahtjeva koji su definirani u ovom dokumentu.

Odgovornosti TSA su specificirane u točki 6.1 ovoga dokumenta.

4.4. Korisnici

Korisnici usluge su pravne ili fizičke osobe koje ugovaraju korištenje usluga izdavanja vremenskog žiga s TSA, kojima je izdan vremenski žig i koje prihvaćaju uvjete pružanja usluga izdavanja vremenskog žiga i svoje obveze i odgovornosti navedene u točki 6.2 ovoga dokumenta.

Kada je korisnik pravna osoba koja obuhvaća nekoliko krajnjih korisnika ili pojedinačnog krajnjeg korisnika, dio obveza navedenih u točki 6.2 ovoga dokumenta preuzimaju krajnji korisnici. Obzirom da je pravna osoba odgovorna ako obveze krajnjih korisnika nisu pravilno ispunjene, očekuje se da pravna osoba informira svoje krajnje korisnike o njihovim obvezama.

Kada je korisnik fizička osoba tada ona odgovora ako obveze i odgovornosti navedene u točki 6.2 ovoga dokumeta nisu pravilno ispunjene.

4.5. Pouzdajuće stane

Pouzdajuće strane su pravne ili fizičke osobe koje primaju vremenski žig i koje djeluju temeljem razumnog pouzdanja u vremenski žig i pružatelja usluga izdavanja vremenskog žiga.

Pouzdajuća strana može ali ne mora biti korisnik.

4.6. AKD TSP/PS

Ovaj dokument „AKD QTSA Pravila i postupci pružanja usluga izdavanja vremenskog žiga (AKD TSP/PS)“ objedinjuje i spaja Pravila pružanja usluga izdavanja vremenskog žiga (*eng. Time-Stamp Policy*)“ koja definiraju ŠTO treba provoditi i Postupke pružanja usluga izdavanja vremenskog žiga (*eng. Practice Statement*)“ koja definiraju KAKO se to provodi.

Ovaj AKD TSP/PS oslanja se i dodatno proširuje AKD-ova pravila i postupke pružanja usluga certificiranja koji su opisani u dokumentima „AKD PKI Opća pravila pružanja usluga certificiranja (CP)“ [23] i „KIDCA Pravilnikom o postupcima certificiranja (CPS)“ [24], a koji su dostupni na AKD-ovom KIDCA portalu na adresi http://id.hr/cps.

Pravila i postupci koji su navedeni u ovom dokumentu oslanjaju se AKD-ovu dokumentaciju sustava upravljanja i interna pravila koja detaljno definiraju tehničke, organizacijske i provedbene postupke koje primjenjuje AKD QTSA. Ovi dokumenti sadrže povjerljive ili tajne poslovne informacije i nisu dostupni javnosti.

5. Uvod u pravila izdavanja vremenskog žiga i osnovni zahtjevi

5.1. Općenito

Pravila i postupci izdavanja vremenskog žiga ispunjavaju zahtjeve norme ETSI EN 319 421 [11], a protokoli vremenskog žiga i profil certifikata TSU jedinica usklađeni su s IETF RFC 3161 [15] te specifikacijama ETSI EN 319 422 [12].

Vremenski žig koji izdaje AKD QTSA ima sljedeća svojstva:

- koristi pouzdani izvor vremena,
- sadrži točan podatak o vremenu koji odgovora vremenu izdavanja vremenskog žiga,
- sadrži podatak o točnosti o UTC vremena koji se ugrađuje u vremenski žig,
- sadrži jedinstveni Identifikator politike izdavanja vremenskih žigova AKD TSA,
- sadrži jedinstveni serijski broj kojim se identificira TST,
- sadrži sažetak (*hash*) informacije za koju se traži vremenski žig s jedinstvenim identifikatorom algoritma koji se koristi za izračun sažetka,
- uključuje podatak koji korisnik šalje u zahtjevu, a koji omogućuje povezivanje zahtjeva za izdavanje vremenskog žiga s TST,
- može biti izdan samo ako je zahtjev za izdavanje vremenskog žiga bio podnesen u ispravnom formatu,
- ne provjerava ispravnost sažetka već samo provjerava odgovara li duljina sažetka duljini koja se očekuje za navedeni algoritam,
- ne uključuje nikakav podatak kojim bi se mogao identificirati pošiljatelj zahtjeva za izdavanje vremenskog žiga,
- potpisan je privatnim ključem TSU jedinice koji se koristi isključivo za potpisivanje vremenskog žiga, a koja je naznačena u ekstenziji certifikata TSU i
- ispunjava sve zahtjeve za izdavanje kvalificiranih vremenskih žigova koji su definirani u članku 42 Uredbe (EU) br. 910/2014 [1].

AKD QTSA koristi TSU jedinice koje isključivo izdaju kvalificirane vremenske žigove. TSU jedinice ne izdaju nekvalificirane vremenske žigove niti se privatni ključ TSU jedinica koriste za bilo koju drugu namjenu osim za pečaćenje kvalificiranih vremenskih žigova.

Kako bi se osigurala kvaliteta i povećala vjerodostojnost usluge izdavanja vremenskog žiga, AKD QTSA postupa sukladno najboljim pravilima struke (eng. Best practices Time-Stamp Policy - BTSP) i normama koje su referencirane u točki 2 ovoga dokumenta tako da podatak o UTC vremenu koji se ugrađuje u vremenski žig ima odstupanje manje od +/- 1 sekundu.

5.2. Identifikacija

Identifikacijska oznaka (OID) koja je pokrivena ovim AKD TSP/PS i po kojoj se izdaje vremenski žig je: 1.3.6.1.4.1.43999.5.7.

Ova pravila ekvivalentna su najboljim pravilima struke za izdavanje vremenskih žigova ETSI BSTP koja se identificiraju oznakom 0.4.0.2023.1.1.

5.3. Zajednica korisnika i primjenjivost

AKD QTSA pruža usluge izdavanja vremenskog žiga za široku javnost i za bilo koju zajednicu korisnika uključujući zatvorene zajednice.

Korisnici i pouzdajuće strane mogu koristiti kvalificirane vremenske žigove koje izdaje AKD QTSA uvijek kada postoji potreba dokazivanje postojanja podataka ili postojanja elektroničkog potpisa podatka u trenutku izdavanja vremenskog žiga odnosno kada postoji potreba za očuvanjem dugotrajnosti elektroničkog potpisa i osiguranja sukladnosti s zahtjevima norme ETSI EN 319 122 [13].
Nije dozvoljena upotreba vremenskog žiga za podatke i sadržaje kojima se krše prava drugih osoba ili se djeluje protivno važećim zakonima ili moralu društva.

5.4. Usklađenost

Prisutnost identifikacijske oznake navedene u točki 5.2 ovoga dokumenta u polju *„Policy"* odgovora na zahtjev za izdavanje vremenskog žiga (vidi točku 7.7.1.3), ukazuje da AKD QTSA primjenjuje pravila i postupke koji su navedeni u poglavlju 7 ovoga dokumenta da i ispunjava svoje obveze koje su navedene u točki 6.1 ovoga dokumenta.

Kako bi demonstrirao svoju usklađenost sa ovim AKD TSP/PS, s Uredbom (EU) br. 910/2014 [1], relevantnim ETSI normama [7], [11] i [12] kao i sa normama ISO/IEC 9001 [22] i ISO/IEC 27001 [19], AKD QTSA je podvrgnut periodičnim internim i vanjskim revizijama te neovisnom ocjenjivanju usklađenosti.

6. Pravila i postupci

6.1. Procjena rizika

AKD provodi procjenu rizika u skladu s normom ISO/IEC 27005 [21] pri čemu se uzimaju u obzir poslovni i tehnički aspekti povezani s pružanjem usluga izdavanja vremenskog, a posebno zahtjevi koji su navedeni u poglavlju 5 norme ETSI EN 319 401 [7].

6.2. Postupci pružanja usluga

Ovaj AKD TSP/PS i AKD CP/CPS na koje se ovaj dokument oslanja dostupni su na AKD-ovom KIDCA portalu na adresi http://id.hr/cps.

Ovaj AKD TSP/PS sadrži sve potrebne informacije koje su definirane u poglavlju 6.2 norme ETSI EN 319 421 [11] kao i u poglavlju 6.1 norme ETSI EN 319 401 [7].

6.3. Uvjeti pružanja usluga izdavanja vremenskog žiga

Prije sklapanja sporazuma s AKD QTSA, korisnici i pouzdajuće strane informirane su o uvjetima pod kojima AKD QTSA pruža usluga izdavanja vremenskog žiga.

Dokument AKD QTSA Opći uvjeti pružanja usluga izdavanja vremenskog žiga (u daljnjem tekstu: AKD TSDS) dostupan je na AKD-ovom KIDCA portalu na adresi http://id.hr/cps.

AKD TSDS sadrži sve potrebne informacije za korisnike pouzdajuće strane kako je zahtijevano u poglavlju 6.2 norme ETSI EN 319 401 [7].

AKD QTSA može naplatiti naknadu za pružanje usluga izdavanja vremenskog žiga.

6.4. Upravljanje informacijskom sigurnošću

Upravljanje informacijskom sigurnošću provodi se u skladu s normom ISO/IEC 27001 [19] i specifičnim zahtjevima koji su definirani u poglavlju 6.3 norme ETSI EN 319 401 [7].

Organizacijski i provedbeni postupci upravljanja informacijskom sigurnošću detaljno su specificirani u AKD-ovim internim pravilima i procedurama.

6.5. Odgovornosti TSA

6.5.1. Općenito

Obveze i odgovornosti pružatelja usluga izdavanja vremenskog žiga, korisnika i pouzdajućih strana proizlaze iz AKD TSDS odnosno ugovora koji se sklapa s korisnicima.

Obveze pružatelja usluga izdavanja certifikata kIDCA koje je izdalo TSU certifikat definirane su u poglavlju 9.6.1. AKD CP/CPS.

Obveze i odgovornosti pružatelja usluga, korisnika i pouzdajućih strana dodatno su utvrđene Zakonom o obveznim odnosima [3], Zakonom o zaštiti potrošača [4] i Direktivom 93/13/EEC [5].

6.5.2. Obveze TSA prema korisnicima

AKD kao pružatelj usluga izdavanja vremenskog žiga se obvezuje:

- da će pružati usluge izdavanja vremenskog žiga u skladu s AKD TSP/PS i AKD TSDS i da će postupati u skladu s AKD CP/CPS koje će objavljivati na portalu http://id.hr/cps,
- da će podatak o UTC vremenu koji se ugrađuje u vremenski žig imati odstupanje manje od +/- 1 sekundu,
- da će osigurati kontinuirani 24/7/365 pristup i maksimalnu dostupnost usluga osim u slučaju planiranih tehničkih radova i okolnosti koje su definirane u točki 6.6 ovog dokumenta.
- da će osigurati stručno osoblje i dostatna financijska sredstva kako bi se osigurala očekivana kvaliteta i kontinuitet pružanja usluge izdavanja vremenskog žiga,
- da će osigurati postupanje u skladu s Uredbom (EU) br. 910/2014 [1] i Zakonom o provedbi Uredbe (EU) br. 910/2014 [2],
- da će provoditi zakonitu obradu i zaštitu osobnih podataka kao i svih zaštitu ostalih povjerljivih poslovnih informacija i
- da će provoditi interne i vanjske revizije te procjene sustava kako bi osigurao sukladnost s regulatornim zahtjevima, ovim AKD TSP/PS kao i ostalim internim pravilima i procedurama AKD-a.

6.5.3. Obveze korisnika

Korisnici se obvezuju:

- da će provjeriti potpis tokena vremenskog žiga (TST),
- da će provjeriti izdavatelja TSU certifikata i valjanost svih certifikata na certifikacijskoj stazi,
- da će provjeriti da TSU certifikat kojim je potpisan TST nije istekao i da nije opozvan u trenutku potpisa TST,

- da će prilikom izrade zahtjeva za izdavanje vremenskog žiga koristiti pouzdane kriptografske funkcije i
- da će informirati krajnje korisnike i pouzdajuće strane o prihvatljivom načinu korištenja usluga izdavanja vremenskog žiga i o uvjetima koji su definirani u AKD TSDS, AKD TSP/PS i AKD CP/CPS.

Svaki odgovor na zahtjev za izdavanje vremenskog žiga sadrži TSU certifikat. Postupak provjere TSU certifikata i certifikacijske staze definiran je u točki 9.6.4 AKD CP/CPS.

Više informacija o tome kako provjeriti TST i kako staviti potpis u određenu točku vremena definirano je u IETF RFC 3161 [15] i njegovom korekcijama u IETF RFC 5816 [16].

6.5.4. Obveze pouzdajućih strana

Pouzdajuće strane se obvezuju:

- da će se prije korištenja usluga informirati o AKD TSDS i AKD TSP/PS, a posebno o svojim odgovornostima i obvezama te prihvatljivom načinu korištenja usluga izdavanja vremenskog žiga,
- da će prije ostvarivanja pouzdanja u TST provjeriti da je TST korektno potpisan i da privatni ključ koji je korišten za potpisivanje TST nije kompromitiran do trenutka validacije vremenskog žiga kako je navedeno u točki 9.6.4 AKD CP/CPS,
- da će za vrijeme perioda važenja TSU certifikata provjeriti status TSU certifikata korištenjem podataka koji su sadržani u TSU certifikatu i
- da će voditi računa o svim ograničenjima i propisanim mjerama predostrožnosti, a posebno u slučaju izrade dugotrajnih vremenskih žigova.

Ako se provjera vremenskog žiga provodi nakon isteka perioda važenja TSU certifikata, pouzdajuće strane trebaju slijediti smjernice navedene u dodatku D norme ETSI EN 319 421 [11].

Pouzdajuće strane trebaju:

- provjeriti da privatni ključ TSU nije bio kompromitiran ni u kojem trenutku do trenutka kada pouzdajuća strana provjerava vremenski žig.
- provjeriti da algoritam koji se koristi za izračun sažetka u vremenskom žigu nije zastario u trenutku provjere vremenskog žiga i
- provjeriti da su duljine kriptografskih ključeva te korišteni algoritmi i parametri još uvijek prikladni za korištenje u trenutku provjere vremenskog žiga.

Održavanje valjanosti vremenskog žiga kroz dugi vremenski period može se postići ponovnom primjenom vremenskog žiga kojim će se zaštititi integritet prethodno izrađenog vremenskog žiga. Prije ponovne primjene vremenskog žiga potrebno je provjeriti i utvrditi da je prethodno izrađeni vremenski žig valjan.

Pouzdajuće strane trebaju biti svjesne da nakon isteka perioda važenja TSU certifikata, certifikacijsko tijelo kIDCA koje je izdalo TSU certifikat više nije dužno obrađivati informacije o statusu isteklih i nevažećih certifikata.

6.6. Izuzeće od daljnje odgovornosti

AKD daje jamstvo za ono što je kao pružatelj usluga izdavanja vremenskog žiga odgovoran, a što je izričito navedeno da je odgovornost AKD-u u točki 6.5.2 ovoga dokumenta.

AKD ima osiguran rizik od odgovornosti za štete koje nastaju pružanjem usluga povjerenja.

Prema osobama i pouzdajućim stranama koje primjereno koriste uslugu izdavanja vremenskog žiga, visina ukupne financijske odgovornosti za transakcije obavljene na temelju pouzdanja u vremenski žig ograničava se na iznos do 80.000 kn.

AKD nije odgovoran za:

- štete koje su prouzročene neprimjerenim korištenjem usluge izdavanja vremenskog žiga,
- štete prouzročene neispravnošću ili pogreškama u softveru ili hardveru korisnika ili pouzdajuće strane,
- štete koje je namjerno ili nepažnjom prouzročio korisnik ili pouzdajuća strana koja ne ispunjava svoje obveze ili ne djeluje u skladu sa svojim obvezama i
- štete koje mogu proizaći iz korištenja vremenskog žiga.

AKD nije odgovoran za bilo koji gubitak koji može nastati kao posljedica djelovanja više sile i ostalih okolnosti koje su izvan kontrole AKD-a uključujući vremenske i prirodne katastrofe, odron zemlje, poplave, požar, eksplozije, rat, ratne zločine, terorizam, upade u fizički prostor, upade u informacijski sustav, građanske nemire, prekide napajanja, kvarove hardvera, softvera ili komunikacijske infrastrukture te ostalih okolnosti koje su izvan kontrole AKD-a.

7. TSA upravljanje i provedba

7.1. Uvod

AKD osigurava da se uspostava, implementacije, održavanja i kontinuiranog unapređenje sustava upravljanja kvalitetom i informacijskom sigurnošću provodi u skladu s najboljim poslovnim praksama i normama.

Detaljnije informacije o fizičkim, organizacijsko upravljačkim i tehničkim mjerama zaštite mogu se naći u točkama 5.1, 5.2 i 6 AKD CP/CPS[24].

7.2. Unutarnja organizacija

AKD je uspostavio sustav odgovornosti i odredio je granice pouzdanja u vremenski žig. Korisnici i pouzdajuće strane informirane se o svojim obvezama i odgovornostima te o uvjetima po kojima AKD pruža usluge izdavanja vremenskog žiga.

Financijsko poslovanje AKD-a je stabilno i AKD QTSA raspolaže dostatnim ljudskim resursima i financijskim sredstvima potrebnim za ispunjenje svojih obveza i nesmetano pružanje usluga u skladu s ovim AKD TSP/PS.

AKD ima ogovarajuću policu osiguranja od odgovornosti kako bi pokrio svoje obveze koje proizlaze iz pružanja usluga povjerenja.

Detaljnije informacije o poslovanju pružatelja usluga mogu se naći u AKD CP/CPS, a posebno u točki 9 ovoga dokumenta.

7.3. Osoblje

AKD primjenjuje principe segregacije zaduženja i ostale organizacijsko-upravljačke mjere zaštite u skladu s poglavljem 5.2 AKD CP/CPS.

Odabir, zapošljavanje, educiranje, provjera i informiranje radnika koji sudjeluju u provedbi aktivnosti izdavanja vremenskog žiga provodi se u skladu s poglavljem 5.3 AKD CP/CPS.

7.4. Upravljanje imovinom

AKD osigurava primjerenu razinu zaštitu imovine koja se koristi za pružanje usluga izdavanja vremenskog žiga. U tu svrhu AKD vodi i održava popis imovine te provodi klasifikaciju podataka.

Kako bi se osigurala adekvatno upravljanje i zaštita imovine te spriječilo neautorizirano otkrivanje, modifikacija, premještanje ili uništavanje informacija koje su pohranjeni na medijima, uspostavljene su sigurnosne mjere u skladu s poglavljem 8 ISO/IEC 27002 [20].

7.5. Prava pristupa

Kako bi se priječio neautorizirani pristup računalnim resursima i mreži primjenjuju se mjere zaštite u skladu s točkama 6.5 i 6.7 AKD CP/CPS.

7.6. Kriptografske kontrole

7.6.1. Općenito

Upravljanje kriptografskim ključevima i HSM uređajima provodi se u skladu s poglavlju 10 norme ISO/IEC 27002 [20], a kako je detaljnije specificirano u točkama 6.1, 6.2, 6.3 i 6.4 AKD CP/CPS[24].

7.6.2. Generiranje TSU ključa

Postupak generiranja TSU ključa provodi autorizirano radnici kojima su dodijeljene uloge povjerenja, u fizički sigurnom okružju u zoni visoke sigurnosti prema definiranoj proceduri i unaprijed pripremljenoj tehničkoj skripti.

Kriptografski ključevi TSU jedinica se generiraju, koriste i čuvaju u HSM uređaju koji demonstrira sukladnost s normom FIPS PUB 140-2 level 3 [7].

Svaka TSU jedinica ima svoj certifikat i koristi svoj kriptografski ključ za potpisivanje vremenskog žiga.

TSU ključ je duljine 2048 bita, RSA algoritam.

Period važenja TSU certifikata je 5 godina. Certifikat je važeći od datuma izdavanja (osnovno polje certifikata *„Valid from“*) do datuma isteka roka perioda važenja (osnovno polje certifikata *„Valid to“*).

Period TSU privatnog ključa je 2 godine kako je definirano u polju *„Private Key Usage Period“* TSU certifikata.

Namjena TSU certifikata definirana je kroz vrijednost ekstenzije *„Key Usage“* koja ima vrijednosti *„Digital Signature“*.

TSU certifikat ima dodatno ekstenziju *„Extended Key Usage“* koja ima vrijednost *„Time Stamping (1.3.6.1.5.5.7.3.8)“*

Ekstenzije *„Key Usage“* i *„Extended Key Usage“* označene su kao kritične ekstenzije.

AKD QTSA vodi računa da su kriptografski algoritmi, duljine kriptografskih ključeva i periodi važenja TSU ključeva tijekom njihovog korištenja usklađeni s preporukama norme ETSI TS 119 312 [14].

7.6.3. *Zaštita TSU privatnog ključa*

Cijelo vrijeme i nakon njihove generacije privatni ključevi TSU jedinica ostaju pohranjeni u HSM uređaju i pod kontrolom barem 2 osobe.

Zaštita privatnog ključa TSU jedinica provodi se u skladu s točkama 6.2, 6.3 i 6.4 AKD CP/CPS[24].

7.6.4. *TSU certifikat*

Javni ključevi TSA jedinica dostupni su korisnicima i pouzdajućim stranama u certifikatu. Certifikate TSU jedinica izdaje certifikacijsko tijelo KIDCA te ih objavljuje na svom portalu http://id.hr/cert.

Informacije za provjeru TSU certifikata i certifikacijske staze dostupne su certifikatu TSU.

Profil TSU certifikata je usklađen s zahtjevima normi ETSI EN 319 422 [12] i IETF RFC 3161 [15] kao i s točkom 7 AKD CP/CPS[24].

Profil TSU certifikata prikazan je u sljedećoj tablici.

Tablica 1: Profil TSU certifikata

Polje	Vrijednost
OSNOVNA POLJA	
Version	X.509 V3
Serial Number	Jedinstven pozitivan broj s entropijom od 32 bit-a
Signature Algorithm	SHA256RSA
Issuer DN	CN = KIDCA, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR
Valid from	utcTime
Valid to	utcTime(Valid from +5 godina
Subject DN	CN = AKD QTSA1, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR CN = AKD QTSA2, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR
Subject Public Key	Javni ključ subjekta, RSA (2048 Bits)
Signature Value	Potpis izdavatelja certifikata
EKSTENZIJE	
Key Usage*	Digital Signature
Extended Key Usage*	Time Stamping (1.3.6.1.5.5.7.3.8)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	Derived using the SHA-1 hash of the public key.
Private Key Usage Period	utcTime(Valid from +2 godine
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://id.hr/cert/kidca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-kidca.id.hr/kidca
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.1.2.2.8 [1,1]Policy Qualifier Info:

	Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.id.hr/kidca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.id.hr/kidca.crl
qcStatements	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://id.hr/cps/KIDCA-pds1-0-en.pdf language=en PdsLocation: url= https://id.hr/cps/KIDCA-pds1-0-hr.pdf language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-eseal (2) (0.4.0.1862.1.6.2)

*Kritična ekstenzija

7.6.5. Izdavanje novih TSU ključeva

Prije isteka perioda važenja TSU privatnog ključa, AKD QTSA će zamijeniti privatni ključ i TSU jedinici će izdati novi certifikat. TSU jedinica će odbiti potpisati vremenski žig ako je istekao period važenja TSU privatnog ključa.

7.6.6. Upravljanje životnim ciklusom kriptografskih uređaja

Primjenjuju se norme i upravljačke funkcije kriptografskog modula kako je definirano u točki 6.2.1 AKD CP/CPS[24].

7.6.7. Kraj životnog ciklusa TSU ključa

Tijekom životnog ciklusa TSU ključeva, AKD QTSA vodi računa da se postupak generiranja i ponovnog izdavanja TSU ključeva provede prije isteka perioda važenja TSU ključeva kako ne bi došlo do zastoja u pružanju usluge.

Prilikom izdavanja novog privatnog TSU ključ, stari TSU privatni ključ se trajno uništava i ne može se više koristiti.

Certifikacijsko tijelo kIDCA koje je izdalo TSU certifikat osigurava da su informacije za provjeru statusa TST certifikata dostupne tijekom perioda važenja TSU certifikata.

7.7. Vremenski žigovi

7.7.1. Izdavanje vremenskog žiga

7.7.1.1. Općenito

Zahtjevi za izdavanje vremenskog žiga šalju se uobičajenim HTTP protokolom kako je opisano u IETF RFC 3161 [15].

Prije slanja zahtjeva korisnici AKD QTSA trebaju se autenticirati korištenjem digitalnog certifikata (two-way TLS) ili drugog autentikacijskog sredstva prema uputama koje su objavljene na AKD QTSA Portalu http://id.hr/tsa.

AKD QTSA sustav neće prihvatiti zahtjev za izdavanje vremenskog žiga ako autentikacija korisnika nije bila uspješna.

AKD QTSA sustav neće izdati vremenski žig ako vrijeme koje koristi TSU nije dobiveno od UTC laboratorija ili ako prilikom sinkronizacije s UTC laboratorijem nije postignuta točnost koja je deklarirana u odgovoru na zahtjev za izdavanje vremenskog žiga.

TSU jedinica koristi namjenski privatni ključ koji se koristi isključivo za pečaćenje vremenskog žiga i koji se može se koristiti samo ako nije opozvan ili nije istekao period njegovog važenja.

7.7.1.2. Zahtjev za izdavanje vremenskog žiga

Zahtjev za izdavanje vremenskog žiga koji šalju korisničke aplikacije mora biti u skladu s točkom 2.4.1 IETF RFC 3161 [15] kao i s ESSCertIDv2 promjenama navedenim u točki 2.1 IETF RFC 5816 [16].

Prema ETSI EN 319 422 [12] svaki zahtjev za izdavanje vremenskog žiga treba sadržavati sljedeća polja:

- *reqPolicy*,
- *nonce* i
- *certReq*.

Prema dodatku A.8 norme ETSI TS 119 312 [14], za izračun sažetka informacije za koju se traži vremenski žig potrebno je koristiti neki od sljedećih algoritama (*hashAlgorithm*):

- *sha-256 (OID: 2.16.840.1.101.3.4.2.1)*
- *sha-384 (OID: 2.16.840.1.101.3.4.2.2)*
- *sha-512 (OID: 2.16.840.1.101.3.4.2.3)*

Profil formata zahtjeva za izdavanje vremenskog žiga naveden je u sljedećoj tablici.

Tablica 2: Profil formata zahtjeva

Polje	Podržane vrijednosti	Opis
Version	v1 (1)	Verzija zahtjeva za izdavanje vremenskog žiga
messageImprint	hashAlgorithm: algoritam sažetka hashedMessage: sažetak podatka	Algoritam sažetka i vrijednost sažetka podatka koji se označava vremenskim žigom.
reqPolicy	1.3.6.1.4.1.43999.5.7	Identifikator politike izdavanja vremenskih žigova
nonce	Cijeli broj	Podatak koji omogućava povezivanje zahtjeva i odgovora
certReq	FALSE (default) TRUE	Zahtjev za dostavom certifikata TSU jedinice

7.7.1.3. Odgovor na zahtjev za izdavanje vremenskog žiga

Odgovor na zahtjev za izdavanje vremenskog žiga kojeg šalje AKD QTSA u skladu je s točkom 2.4.2 IETF RFC 3161 [15] kao i s ESSCertIDv2 promjenama navedenim u točki 2.2 IETF RFC 5816 [16].

Prema ETSI EN 319 422 [12] svaki odgovor zahtjev sadrži sljedeća polja:

- *accuracy* i

- *nonce*.

U odgovoru na zahtjev za izdavanje elektroničkih vremenskih žigova polje *nonce* sadrži istu vrijednost koja je stavljena u istoimenom polju zahtjeva za izdavanje vremenskog žiga.

Odgovor na zahtjev za izdavanje vremenskog žiga pečaćen je od strane TSU jedinice.

Prema dodatku A.8 norme ETSI TS 119 312 [14], algoritam koji se koristi za potpisivanje tokena vremenskog žiga TST (*signatureAlgorithm*) je:

- *sha256-with-rsa (OID: 1.2.840.113549.1.1.11)*

Profil formata odgovora na zahtjev za izdavanje vremenskog žiga naveden je u sljedećoj tablici.

Tablica 3: Profil formata odgovora

Polje	Podržane vrijednosti	Opis
PKIStatusInfo	0 (TST je sadržan u odgovoru) 1 (TST je sadržan u odgovoru) Other value (TST nije sadržan u odgovoru)	Informacija o statusu uspješnosti izdavanja vremenskog žiga
TimeStampToken		
version	v1 (1)	Verzija odgovora na zahtjev za izdavanje vremenskog žiga
policy	1.3.6.1.4.1.43999.5.7	Identifikator politike izdavanja vremenskih žigova
serialNumber	Integer	Jedinstveni identifikator TST
genTime	UTC time YYYYMMDDHHMMSS(.s...)Z	Vrijeme u kojem je kreiran TST koje uključuje sekunde
accuracy	1 sekunda	Točnost vremena
nonce	Cijeli broj, duljine 64 bita	Podatak iz zahtjeva koji omogućava povezivanje zahtjeva i odgovora (ako je dostavljen u zahtjevu)

7.7.2. Sinkronizacija vremena s UTC

AKD QTSA posjeduje satelitske prijamnike koji putem GPS satelitskog sustava preuzimaju signal točnog UTC vremena kojeg distribuiraju brojni UTC(k) laboratoriji širom svijeta.

Podatak o UTC vremenu kojeg AKD QTSA ugrađuje u vremenski žig ima odstupanje manje od +/- 1 sekundu.

Kako bi se postigla deklarirana točnost UTC vremena poduzimaju su sljedeće tehničke i organizacijske mjere zaštite:

a) kalibracija satova TSU jedinica provodi se po potrebi, a barem jedan puta dnevno,
b) sustav vodi računa o skokovima od jedne sekunde koji primjenjuje UTC („leap second"),
c) sustav detektira gubitak sinkronizacije s UTC i neće izdati vremenski žig ako odstupanje vremena veće od deklarirane točnosti i
d) sustav bilježi sve aktivnosti i alarmira u slučaju pojave greške, uključujući svako odstupanje od deklarirane točnosti ili nemogućnost kalibriranja satova.

7.8. Fizička sigurnost i sigurnost okružja

AKD QTSA sustav je smješten u poslovnom kompleksu AKD-a u istom prostoru gdje je smješten AKD PKI infrastruktura i KIDCA sustav koji izdaje TSU certifikat.

Primjenjuju se mjere fizičke sigurnosti opisane u točki 5.1 AKD CP/CPS[24].

7.9. Sigurnost provedbe

Informacijski sustav AKD QTSA dio je cjelokupne AKD PKI infrastrukture i primjenjuju se iste kontrole nad računalnim resursima i životnim ciklusom softvera opisanim u točkama 6.5 i 6.6 AKD CP/CPS[24].

AKD QTSA sustav zasnovan je na pouzdanim hardverskim i softverskim komponentama, a sve kritične operacije sustava podržane su redundantnim komponentama.

Primjenjuju se specifične mjere nadzora i upravljanja kapacitetima kako bi se osigurala adekvatna učinkovitost i raspoloživost AKD QTSA sustava.

7.10. Sigurnost mreže

Računalni resursi AKD QTSA odijeljeni su u mrežne zone koje se štite odgovarajućim fizičkim, tehničkim i proceduralnim mjerama zaštite.

Kako bi se osigurala visoka dostupnost usluge i izbjegao zastoj zbog greške ili kvara pojedine komponente sustava, sva mrežna infrastruktura podržana je redundantnim komponentama.

Detaljnije informacije mogu se naći u točki 6.7 AKD CP/CPS[24].

7.11. Upravljanje incidentima

Informacije i radu AKD QTSA sustava prikupljaju se i analiziraju u realnom vremenu tako da se sve neuobičajene i sumnjive aktivnosti automatski alarmiraju.

Upravljanje incidentima i kvarovima računalnih resursa i mreže provodi se po postupcima koji su definirani u točkama 5.7.1 i 5.7.2 AKD CP/CPS[24].

7.12. Upravljanje revizijskim zapisima

Postupci vezani uz prikupljanje, obradu i zaštitu revizijskih zapisa provode se na način opisan u točki 5.4 AKD CP/CPS[24].

Pored toga, bilježe se specifične aktivnosti vezane uz rad AKD QTSA sustava što uključuje ali se ne ograničava na:

a) aktivnosti vezane uz generiranje i životni ciklus TSU ključeva i TSU certifikata,
b) aktivnosti vezane uz sinkronizaciju TSU s UTC vremenom uključujući regularno kalibriranje satova,
c) aktivnosti vezne uz upotrebu TSU privatnog ključa i izdavanje vremenskog žiga i
d) kvarove i ispade sustava uključujući gubitak sinkronizacije ili nemogućnost kalibriranja satova.

Prikupljeni revizijski zapisi arhiviraju se kroz period od 10 godina nakon njihovog nastanka, prema poslovnoj praksi koju primjenjuje AKD i koja je detaljno opisana u točki 5.5 AKD CP/CPS[24].

Svi revizijski zapisi AKD QTSA sustava adekvatno su zaštićeni i vjerodostojni kako bi se mogli prezentirati kao materijalni dokazi u kasnijim eventualnim sudskim postupcima.

7.13. Upravljanje kontinuitetom poslovanja

Primjenjuju se postupci upravljanja kontinuitetom poslovanja prema točki 5.7 AKD CP/CPS[24].

Pored toga primjenjuju se postupci koji su specifični za AKD QTSA koji uključuju:

a) U slučaju kompromitacije ili sumnje u kompromitaciju TSU privatnog ključa, AKD QTSA će trenutno prestati koristiti kompromitirani ključ za potpisivanje TST te će opozvati TSU certifikat.

b) Ako se TSU jedinica nije uspjela sinkronizirani kroz period koji je dulji od jednog dana, TSU će prestati izdavati vremenske žigove sve dok se ne poduzmu potrebne aktivnosti za oporavak sustava.

c) AKD QTSA će putem portala informirati korisnike i pouzdajuće strane o svim gubitcima kalibracije i o svim zastojima u pružanju usluge izdavanja vremenskog žiga.

d) Ako je naknadno utvrđeno da je TSU izdao vremenski žig u kompromitirajućim okolnostima kada je došlo do odstupanja od deklarirane točnosti vremena, AKD QTSA će putem svog portala informirati korisnike i pouzdajuće strane o serijskim brojevima TST za koje postoji sumnja ili koji sadrže neispravne podatke.

7.14. Prestanak rada TSA

Prekid pružanja usluga izdavanja vremenskog žiga provoditi će se u skladu s AKD CP/CPS i donesenim kID planom prekida pružanja usluga certificiranja.

Pored toga, u slučaju prestanka rada AKD QTSA će:

a) pravovremeno informirati nadzorna tijela, korisnike i pouzdajuće strane o namjeri prestanka pružanja usluga izdavanja vremenskog žiga,

b) opcionalno, omogućiti korisnicima nastavak pružanja usluga izdavanja vremenskog žiga kod drugih pružatelja usluga i

c) opozvati certifikate svih TSU jedinica koje koristi za pružanje usluge izdavanja vremenskog žiga.

7.15. Usklađenost sa zakonskim popisima

AKD QTSA osigurava adekvatne dokaze da je poslovna praksa koju provodi sukladna sa primjenjivom zakonskom regulativom.

To se posebno odnosi na sljedeće:

a) prikupljanje minimalnog skupa osobnih identifikacijskih podataka koji su dostatni da se omogući pristup usluzi izdavanja vremenskog žiga

b) jamstvo privatnost te zakonita obrada i zaštita svih osobnih podatka svih korisnika

c) adekvatna zaštita svih povjerljivih poslovnih podataka koji su prikupljeni ili koji nastaju tijekom pružanja usluga izdavanja vremenskog žiga.

AKD QTSA usluga izdavanja vremenskog žiga dostupna je svim osobama koje mogu koristiti internet. Nema posebnih ograničenja za osobe s invaliditetom.

8. Usklađenost s Uredbom (EU) br. 910/2014

AKD QTSA je kvalificirani pružatelj usluga koji izdaje kvalificirani elektronički vremenski žig po Uredbi (EU) br. 910/2014 [1] i relevantnim ETSI normama [7], [11] i [12].

Certifikati AKD TSU jedinica koje pečate vremenske žigove su kvalificirani, a izdaje ih KIDCA certifikacijsko tijelo koje djeluje u skladu s ETSI EN 319 411-1 [9] i ETSI EN 319 411-2 [10].
Korisnici i pouzdajuće strane mogu koristiti pouzdani popis kako bi potvrdili da su AKD TSU i vremenski žig kojeg izdaje AKD QTSA kvalificirani.
Prema ETSI EN 319 421 [11], ako se javni ključ TSU jedinice nalazi na pouzdanom popisu i ako je usluga koju on predstavlja kvalificirana usluga izdavanja vremenskog žiga, tada se vremenski žig koji izdaje ta TSU jedinica može smatrati kvalificiranim.