REKONO Sistemske integracije d.o.o.
A: Ukmarjeva ulica 2, 1000 Ljubljana
www.rekono.si E: info@rekono.si
D. ŠT: SI60762802 MAT ŠT. 8452326

REKONOSIGN
Podjetje: Rekono, sistemske integracije, d.o.o.
Podpisnik: MIHA POBERAJ
Izdajatelj: RekonoSign RSA QC CA3
Datum: 19.11.2024 16:31

Ponudnik storitev zaupanja Rekono TSP; Pravila delovanja za kvalificirano storitev potrjevanja veljavnosti elektronskih podpisov in elektronskih žigov (Rekono QSVS Pravila delovanja)

Verzija:	1.0
Datum izdaje:	19. november 2024
Datum uveljavitve:	01. januar 2025

Zaščita dokumenta

© podjetje Rekono d.o.o.
Vse pravice pridržane. Reprodukcija po delih ali v celoti na kakršenkoli način in v kateremkoli mediju ni dovoljena brez pisnega dovoljenja avtorja. Kršitve se sankcionirajo v skladu z avtorsko pravno in kazensko zakonodajo.

Nadzor različic dokumenta

Izvirni dokument je shranjen v elektronski obliki, različice dokumenta so pod nadzorom. Morebitne papirne ali elektronske kopije tega dokumenta lahko obstajajo za namene razdeljevanja tistim, ki jim je dokument namenjen oz. se morajo z njim seznaniti v okviru izvajanja delovnih nalog. Kopije dokumenta niso nadzorovane in jih mora bralec obravnavati kot take.

Zgodovina sprememb dokumenta:

Datum	Različica	Opis / opomba
19.11.2024	1.0	Prva verzija

Kazalo

1. Uvod ... 6
1.1. Pregled ... 6
1.1.1. Identifikacija ponudnika storitev zaupanja ... 6
1.1.2. Podprta politika za storitev potrjevana veljavnosti podpisov ... 7
1.2. Komponente storitve preverjanja veljavnosti podpisa ... 7
1.2.1. Sodelujoči subjekti ... 7
1.2.2. Arhitektura storitve ... 7
1.3. Definicije in okrajšave ... 8
1.3.1. Definicije ... 8
1.3.2. Okrajšave ... 11
1.4. Politike in postopki ... 13
1.4.1. Organizacija, ki upravlja s pričujočim dokumentom ... 13
1.4.2. Kontaktni podatki ... 13
1.4.3. Javni dokumenti ponudnika storitve zaupanja ... 13
2. Upravljanje in delovanje storitve zaupanja ... 14
2.1. Interna organizacija ... 14
2.1.1. Zanesljivost zunanje organizacije ... 14
2.1.2. Ločevanje dolžnosti ... 14
2.2. Osebje ... 15
2.2.1. Kvalifikacije, izkušnje in varnostno preverjanje ... 15
2.2.2. Usposabljanje osebja ... 15
2.2.3. Pogostost dodatnih usposabljanj ... 15
2.2.4. Ukrepi ob kršitvah pooblastil ... 15
2.2.5. Zahteve za pogodbene izvajalce ... 15
2.3. Upravljanje s sredstvi ... 16
2.3.1. Splošne zahteve ... 16
2.3.2. Ravnanje z mediji ... 16
2.4. Nadzor dostopa ... 16
2.5. Upravljanje kriptografskih ključev ... 16
2.6. Fizično varovanje ... 16
2.7. Operativno upravljanje varnosti sistemov ... 16
2.8. Varnostne kontrole na ravni računalniškega omrežja ... 17
2.9. Postopki za odzivanje na varnostne incidente in nepravilnosti ... 17
2.10. Zbiranje dokazov ... 17
2.11. Upravljanje kontinuitete poslovanja ... 17
2.12. Prenehanje delovanja ponudnika storitev ... 17
2.13. Preverjanje skladnosti in ostale oblike nadzora ... 18
3. Tehnične lastnosti storitve potrjevanja veljavnosti podpisa ... 19
3.1. Postopek potrjevanja veljavnosti podpisa ... 19

3.2. Protokol potrjevanja veljavnosti podpisa 20
3.3. Vmesniki 20
3.3.1. Komunikacijski kanal 20
3.3.2. Ponudnik storitve potrjevanja podpisov – ostali ponudniki storitev zaupanja 20
3.4. Poročilo o potrditvi veljavnosti podpisa 20
4. Dodatki 22
4.1. Reference 22

1. Uvod

1.1. Pregled

V okviru podjetja Rekono d.o.o. deluje ponudnik storitev zaupanja Rekono TSP, ki deluje kot ponudnik storitev zaupanja za kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov, za kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov in druge storitve zaupanja, kot so overjanje digitalnih potrdil za kvalificirani elektronski podpis, kvalificirani elektronski žig, napredni elektronski podpis, napredni elektronski žig, elektronsko avtentikacijo in izdajanje kvalificiranih elektronskih časovnih žigov.

Rekono TSP deluje kot javni ponudnik storitev zaupanja v skladu z UREDBO (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.

Pričujoči dokument, Rekono TSP Pravila delovanja za kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov in kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov (v nadaljevanju Rekono QSVS Pravila delovanja), vsebuje pogoje uporabe in opis pravil ter postopkov, ki jih izvaja Rekono d.o.o. za izvajanje potrjevanja veljavnosti kvalificiranih elektronskih podpisov in kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov. Rekono QSVS Pravila delovanja vsebujejo poleg navedenega tudi opis tehničnih lastnosti in operativnih postopkov upravljanja infrastrukture IT, ki jo Rekono d.o.o. uporablja za izvajanje in upravljanje storitve potrjevanja veljavnosti kvalificiranih elektronskih podpisov in kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov.

Rekono TSP izvaja kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov, za kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov (krajše Rekono QSVS) v skladu s členi 32, 33 in 40 Uredbe eIDAS.

Vsebina in oblika Rekono QSVS Pravil delovanja sledi obliki in zahtevam ETSI TS 119 441: Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

Definicije in okrajšave, uporabljene v pričujočem dokumentu, so povzete po uredbi eIDAS [6] in ETSI TR 119 001 [7]. Glej tudi 1.3.

1.1.1. Identifikacija ponudnika storitev zaupanja

Storitve zaupanja po pričujočem dokumentu, Rekono QSVS Pravila delovanja, izvaja Rekono, sistemske integracije, d.o.o. (kratko ime Rekono d.o.o.).

Podatki Rekono d.o.o. vpisani v Poslovni register Slovenije:

Polno ime:	Rekono, sistemske integracije, d.o.o.
Kratko ime:	Rekono d.o.o.
Naslov:	Ukmarjeva ulica 2

Naselje: Ljubljana
Pošta: 1000 Ljubljana
Matična številka: 8452326000
Davčna številka: SI 60762802

1.1.2. Podprta politika za storitev potrjevana veljavnosti podpisov

Rekono TSP storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov in potrjevanja veljavnosti kvalificiranih elektronskih žigov (krajše Rekono QSVS) se izvaja v skladu s politiko z OID 0.4.0.19441.1.2, opredeljeno v ETSI TS 119 441 [30], poglavje 4.2.2.

0.4.0.19441.1.2	itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)

1.2. Komponente storitve preverjanja veljavnosti podpisa

1.2.1. Sodelujoči subjekti

Subjekta, ki neposredno sodelujeta v postopku potrjevana veljavnosti podpisov, sta ponudnik storitev zaupanja in naročnik.

Ponudnik storitev zaupanja upravlja in ponuja storitev potrjevanja veljavnosti podpisov.

Naročnik (tudi uporabnik) je aplikacija ali fizična oseba, ki komunicira s sistemom za preverjanje veljavnosti podpisa, ki ga upravlja in ponuja ponudnik storitev zaupanja.

Drugi subjekti, ki so lahko posredno del postopka potrjevana veljavnosti podpisov, so:

- kvalificirani ponudnik storitev zaupanja, ki je izdal podpisno potrdilo;
- kvalificirani ponudnik storitev zaupanja, ki je izdal elektronski časovni žig;
- izdajatelji zaupanja vrednih seznamov evropskih držav članic;
- Evropska komisija, ki zagotavlja seznam zaupanja vrednih seznamov.

1.2.2. Arhitektura storitve

Storitev potrjevanja veljavnosti podpisov sestavljata dva osnovna modula – uporabniški vmesnik in zaledni sistem.

Uporabniški vmesnik omogoča dostop do storitve preko spletnega grafičnega vmesnika ali aplikacijskega programskega vmesnika.

Zaledni sistem oziroma zaledna aplikacija za potrjevanje veljavnosti podpisov izvaja funkcije potrjevanja veljavnosti podpisanih in/ali časovno žigosanih dokumentov, in sicer:

- Preverjanje, da dokument ni bil spremenjen;
- Preverjanje oblike podpisa;

- Preverjanje veljavnosti potrdila, to je, da potrdilo ni poteklo, ni preklicano ali začasno preklicano;
- Preverjanje, da je podpisno potrdilo izdal kvalificirani ponudnik storitev zaupanja in da je status ponudnika na zaupanja vrednem seznamu veljaven (LOTL);
- Preverjanje, da je elektronski časovni žig, če ga dokument vsebuje, veljaven in da ga je izdal kvalificirani ponudnik storitev zaupanja in da je status ponudnika na zaupanja vrednem seznamu veljaven (LOTL);
- Ustvari poročilo o preverjanju veljavnosti podpisa;
- Ožigosa poročilo z naprednim elektronskim žigom storitve Rekono QSVS.

Za prenos podatkov se uporablja protokol TLS.

Med obdelavo oziroma postopkom preverjanja veljavnosti podpisa se podatki obdelujejo v sistemskem pomnilniku aplikacijskega strežnika in niso fizično shranjeni na datotečnem sistemu (niti kot začasni podatki) ali v podatkovni zbirki. Po postopku preverjanja se podatki izbrišejo iz pomnilnika.

Celoten postopek preverjanja se beleži.

1.3. Definicije in okrajšave

1.3.1. Definicije

Splošne definicije so povzete po eIDAS [6] in ETSI TR 119 001 [7]:

Digitalni podpis	Je kriptografska preobrazba niza podatkov ali dodan niz podatkov, ki omogoča prejemniku dokazovanje vira in celovitosti podatkov ter zaščito pred ponarejanjem, npr. s strani prejemnika.
Elektronski podpis	Je niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani in jih podpisnik uporablja za podpisovanje.
Napredni elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: a) enolično je povezan s podpisnikom; b) z njim je mogoče identificirati podpisnika; c) ustvari se na podlagi podatkov za ustvarjanje elektronskega podpisa, ki jih podpisnik z visoko stopnjo zaupanja lahko uporablja izključno pod svojim nadzorom, in

	d) s podatki, ki so na ta način podpisani, je povezan tako, da je opazna vsaka naknadna sprememba podatkov.
Potrdilo za elektronski podpis	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe.
Elektronski žig	Pomeni niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov.
Napredni elektronski žig	Je elektronski žig, ki izpolnjuje naslednje zahteve: a) enolično je povezan z ustvarjalcem žiga; b) z njim je mogoče identificirati ustvarjalca žiga; c) ustvari se na podlagi podatkov za ustvarjanje elektronskega žiga, ki jih ustvarjalec žiga z visoko stopnjo zaupanja in pod svojim nadzorom lahko uporablja za ustvarjanje elektronskega žiga, in d) povezan je s podatki, na katere se nanaša, in sicer tako, da je mogoče zaslediti vsako naknadno spremembo teh podatkov.
Ustvarjalec žiga	Pomeni pravno osebo, ki ustvari elektronski žig.
Podatki za ustvarjanje elektronskega žiga	Pomenijo enolične podatke, ki jih ustvarjalec elektronskega žiga uporabi za ustvarjanje elektronskega žiga.
Potrdilo za elektronski žig	Pomeni elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe.
Informacijski sistem	Je sistem za oblikovanje, pošiljanje, prejemanje, shranjevanje in druge obdelave podatkov v elektronski obliki.

Potrdilo javnega ključa	Je javni ključ imetnika, skupaj z nekaterimi drugimi informacijami postane digitalno podpisan z zasebnim ključem overitelja, ki ga je izdal.
Digitalno potrdilo	Glej "Potrdilo javnega ključa".
Potrdilo	Sinonim za potrdilo javnega ključa oziroma digitalno potrdilo.
Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njuna specifična sestavina, ki jo ponudnik storitev zaupanja uporablja za storitve v zvezi z elektronskim podpisovanjem oz. se uporablja za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem digitalnih potrdil. V kontekstu Uredbe eIDAS deluje overitelj v okviru ponudnika storitev zaupanja.
Podatki za ustvarjanje elektronskega podpisa	Pomeni enolične podatke, ki jih podpisnik uporablja za ustvarjanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je fizična oseba, ki ustvari elektronski podpis.
Ponudnik storitev zaupanja	Pomeni fizično ali pravno osebo, ki zagotavlja eno ali več storitev zaupanja kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja, ki so opredeljene v Uredbi eIDAS.
Kvalificirana storitev zaupanja	Pomeni storitev zaupanja, ki izpolnjuje zadevne zahteve Uredbe eIDAS [6].
Sredstvo za elektronsko podpisovanje	Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz Zakona o elektronskem poslovanju in elektronskem podpisu.
Sredstvo za preverjanje elektronskega podpisa	Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.

Naročnik (ang. Subscriber)	Fizična oseba ali poslovni subjekt, ki zahteva dostop do storitve oziroma jo uporablja.
Korenski overitelj	Izdajatelj digitalnih potrdil, ki v okviru overiteljeve infrastrukture javnih ključev predstavlja izhodišče zaupanja (angl. trust point). Korenski izdajatelj se uporablja le za izdajo digitalnih potrdil podrejenim izdajateljem.
Podrejeni overitelj	Izdajatelj digitalnih potrdil, ki mu je digitalno potrdilo izdal korenski oziroma nadrejeni izdajatelj. Podrejeni izdajatelj izdaja digitalna potrdila naročnikom oziroma končnim uporabnikom ali drugim podrejenim izdajateljem.
Poslovni subjekt	Fizične in pravne osebe, ki opravljajo poslovno dejavnost.
Organizacija	Sinonim za poslovni subjekt.
Uporabnik potrdila	Sinonim za imetnika potrdila.
Elektronski časovni žig	Pomeni podatke v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali.
Kvalificirani elektronski časovni žig	Pomeni elektronski časovni žig, ki izpolnjuje zahteve iz člena 42 uredbe eIDAS.
Podatki za potrjevanje veljavnosti	Pomeni podatke, ki se uporabljajo za potrjevanje veljavnosti elektronskega podpisa ali elektronskega žiga.
Potrjevanje veljavnosti	Pomeni postopek preverjanja in potrditve, da so podatki v elektronski obliki veljavni v skladu z Uredbo eIDAS.

1.3.2. Okrajšave

ASN.1	Abstract Syntax Notation One
CA	Certification Authority
PKI	Public Key Infrastructure
CRL	Certificate Revocation List (seznam preklicanih digitalnih potrdil)
OID	Object IDentifier

URI	Uniform Resource Identifier
URL	Uniform Resource Locator
RDN	Relative Distinguished Name
CN	Common Name
DN	Distinguished Name (razločevalno ime)
PMA	Policy Management Authority
HSM	Hardware Security Module (strojni varnostni modul)
DMZ	Demilitarized Zone
IPS	Intrusion prevention system
OCSP	Online Certificate Status Protocol
POE	Projektna organizacijska enota
TSP	Trust Service Provider (ponudnik storitev zaupanja)
NTP	Network time protocol
BIMP	Bureau International des Poids et Mesures (https://www.bipm.org)
UTC	Coordinated Universal Time
TSA	Time-stamp authority
OI	Organization Identifier (polje organizationIdentifier v razločevalnem imenu potrdila)
LOTL	List of Trusted Lists (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml)
AdES	Napredni elektronski podpis ali žig
QES	Kvalificirani elektronski podpis ali kvalificirani elektronski žig
QESig	Kvalificirani elektronski podpis
QESeal	Kvalificirani elektronski žig
AdESig-QC	Napredni elektronski podpis, ki temelji na kvalificiranem potrdilu
AdESeal-QC	Napredni elektronski žig, ki temelji na kvalificiranem potrdilu
API	Aplikacijski programski vmesnik
SVS	Storitev potrjevanja veljavnosti podpisov (en. Signature Validation Service)
QSVS	Kvalificirana storitev potrjevanja veljavnosti podpisov (en. Qualified Signature Validation Service)

1.4. Politike in postopki

1.4.1. Organizacija, ki upravlja s pričujočim dokumentom

Z dokumentom upravlja podjetje Rekono d.o.o.

1.4.2. Kontaktni podatki

Naslov:	Rekono d.o.o. Ukmarjeva ulica 2 1000 Ljubljana
E-mail:	info@rekono.si
Internet:	https://www.rekono.si

1.4.3. Javni dokumenti ponudnika storitve zaupanja

Vsi postopki in aktivnosti, ki jih izvaja ponudnik storitev Rekono TSP za opravljanje storitve Rekono QSVS, so opisani v pričujočem dokumentu Rekono QSVS Pravila delovanja, ki je javno dostopen na javni spletni strani ponudnika storitev zaupanja Rekono d.o.o.

Rekono QSVS Pravila delovanja oziroma novo različico odobri zakoniti zastopnik podjetja Rekono d.o.o. Dokument se odobri in objavi v elektronski različici v obliki PDF. Odobritev oziroma podpis se izvede s kvalificiranim elektronskim podpisom zakonitega zastopnika.

2. Upravljanje in delovanje storitve zaupanja

2.1. Interna organizacija

Rekono d.o.o. ima za upravljanje in izvajanje storitev zaupanja Rekono TSP projektno organizacijsko strukturo s tremi projektnimi organizacijskimi enotami (POE):

- Rekono.PMA - POE za upravljanje storitev zaupanja (angl. Policy Management Authority – PMA)
- Rekono.OA - POE za operativno delovanje storitev zaupanja (angl. Operations Authority – OA)
- Rekono.RA – POE za registracijo (angl. Registration Authority – RA)

Osebe, ki izvajajo naloge posamezne POE, so stalno zaposleni, začasno zaposleni ali osebe, ki imajo z Rekono d.o.o. pogodbo o izvajanju zadevnih storitev.

Rekono d.o.o. ima sklenjeno pogodbo z OSI d.o.o., Ukmarjeva ulica 2, Ljubljana za izvajanje storitev v okviru nalog Rekono.PMA in Rekono.OA.

2.1.1. Zanesljivost zunanje organizacije

Rekono d.o.o. ima za izvajanje nekaterih dejavnosti sklenjene pogodbe z zunanjimi izvajalci. To je na primer za razvoj programske opreme, vzdrževanje sistemske programske opreme, pravne zadeve, revizije itd. Ti subjekti so dolžni upoštevati ustrezna pravila delovanja in splošne pogoje ponudnika storitev zaupanja Rekono d.o.o. in dotično zakonodajo.

Podjetje Rekono d.o.o. v celoti odgovarja za dejanja svojih zunanjih izvajalcev.

2.1.2. Ločevanje dolžnosti

Rekono TSP ima opredeljeno organizacijsko strukturo, razdelitev nalog ter pooblastil za dostop do infrastrukture in podatkov glede na naloge, ki jih opravlja posamezna oseba.

Osebje Rekono TSP ima operativne vloge za opravljanje zaupanja vrednih nalog razdeljene v sledeče skupne:

- Osebe zadolžene za upravljanje strojnih varnostnih modulov (HSM) in logičnih particij HSM. Zadolžitve so razdeljene v sledeče skupine:
  - Varnostni skrbnik HSM
  - Administrator HSM
  - Varnostni skrbnik logične particije HSM
  - Uporabnik logične particije HSM
- Osebe zadolžene za upravljanje nastavitev programske opreme ter dodajanje in upravljanje pooblastil oseb zadolženih za operativno upravljanje posamezne storitve zaupanja.
- Osebe zadolžene za operativno upravljanje posamezne storitve zaupanja.

- Osebe zadolžene za hrambo varnostnih kopij kriptografskih ključev storitev Rekono TSP in po potrebi drugih varnostno občutljivih podatkov.
- Osebe zadolžene za upravljanje sistemov IT, na katerih delujejo sklopi programske opreme storitev Rekono TSP.

Rekono TSP zagotavlja delitev dolžnosti operativnega osebja in s tem nezdružljivost nalog z dodelitvijo zgoraj navedenih zaupanja vrednih nalog različnim osebam.

V primeru, ko ima posamezna oseba več zaupanja vrednih vlog, se za avtentikacijo uporablja princip štirih oči (angl. Four Eyes Principle, also Two-man rule).

2.2. Osebje

2.2.1. Kvalifikacije, izkušnje in varnostno preverjanje

Rekono TSP dodeljuje zaupanja vredne operativne vloge zaposlenim in po potrebi zunanjim izvajalcem. Primernost posameznika za določeno operativno vlogo potrdi oziroma odobri Rekono.PMA.

Člani osebja ne smejo izvajati nalog, ki so v nasprotju interesov z njihovo vlogo v okviru Rekono TSP.

2.2.2. Usposabljanje osebja

Člani osebja Rekono TSP imajo, poleg ustrezne formalne izobrazbe, tudi opravljena dodatna interna ali zunanja izobraževanja in/ali delovne izkušnje glede na specifičnost njihov nalog.

2.2.3. Pogostost dodatnih usposabljanj

Zahteve za usposabljanje osebja so redno pregledane in posodobljene, kadar je to zahtevano za prilagoditev spremembam glede na spremembe tehnologije in različic programske opreme.

2.2.4. Ukrepi ob kršitvah pooblastil

Nepooblaščena dejanja ali prekrški se obravnavajo kot incident in kršitev pravilnika o varovanju poslovnih skrivnosti v skladu z internimi akti Rekono d.o.o.

2.2.5. Zahteve za pogodbene izvajalce

Osebe, ki izvajajo naloge, so lahko pogodbeni izvajalci, ki imajo z Rekono d.o.o. pogodbo o izvajanju zadevnih storitev.

Kjer so za naloge potrebni zunanji izvajalci, je izvedeno preverjanje usposobljenosti izvajalcev. Vsi pogodbeni izvajalci morajo podpisati sporazum o varovanju in nerazkrivanju zaupnih podatkov.

2.3. Upravljanje s sredstvi

2.3.1. Splošne zahteve

Podjetje Rekono d.o.o., ki izvaja storitev zaupanja Rekono TSP, ima vzpostavljen sistem upravljanja informacijske varnosti v skladu z ISO/IEC 27001 in upravljanja informacijskih storitev v skladu z ISO/IEC 20000. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001 in ISO/IEC 20000.

2.3.2. Ravnanje z mediji

Mediji, na katerih se hranijo elektronski zapisi in varnostne kopije občutljivih podatkov, se hranijo v dveh varnostnih omarah.

2.4. Nadzor dostopa

Glej 2.6.

2.5. Upravljanje kriptografskih ključev

Zasebni podpisni kriptografski ključi storitev, ki se uporabljajo za digitalno podpisovanje v okviru storitve zaupanja Rekono QSVS, so ustvarjeni v strojnih varnostnih modulih (angl. Hardware Security Module, HSM) v okviru nadzorovanega postopka (angl. Key Generation Ceremony). Postopek se izvede v nadzorovanem okolju pod nadzorom več oseb v skladu s priporočili in prakso za generiranje kriptografskih ključev ponudnikov storitev zaupanja.

Generiranje kriptografskih ključev za ustvarjanje naprednega elektronskega žiga storitve Rekono QSVS se izvaja v strojnih varnostnih modulih, ki imajo potrdilo o skladnosti s FIPS 140-2 Level 3.

2.6. Fizično varovanje

Varnostni ukrepi na nivoju fizičnega okolja so opisani v interni dokumentaciji ponudnika storitev Rekono d.o.o. Dokumentacija oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

2.7. Operativno upravljanje varnosti sistemov

Strojna in programska oprema, ki jo uporablja Rekono TSP, so standardni (angl. off-the-shelf) produkti, ki so dodatno varnostno okrepljeni po priporočilih CIS Benchmarks (https://www.cisecurity.org/cis-benchmarks/).

Varnostni ukrepi na nivoju sistemov, ki jih Rekono TSP uporablja za izvajanje storitev, so opisani v interni dokumentaciji ponudnika storitev Rekono d.o.o. Dokumentacija

oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001 in ISO/IEC 20000.

2.8. Varnostne kontrole na ravni računalniškega omrežja

Računalniška mreža, v kateri so nameščeni sistemi ponudnika storitev zaupanja, je razdeljena na več segmentov. Ločevanje in nadzor mrežnega prometa med segmenti se zagotavlja z uporabo požarnih zidov. Do posameznih segmentov in strežnikov je dovoljen samo eksplicitno specificiran mrežni promet nujno potreben za posamezno storitev.

2.9. Postopki za odzivanje na varnostne incidente in nepravilnosti

Ponudnik storitev zaupanja Rekono d.o.o. izvaja postopke za odzivanje na varnostne incidente in nepravilnosti v skladu z ISO/IEC 27001. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

2.10. Zbiranje dokazov

Zapisi za vsako preverjaje veljavnosti podpisa se zbirajo in hranijo v zbirki revizijskih sledi. Vsak zapis ima časovno oznako in kontrolo integritete. Zapisi v zbirki revizijskih sledi se hranijo vsaj 10 let.

2.11. Upravljanje kontinuitete poslovanja

Rekono TSP ima vzpostavljeno storitev na več ločenih lokacijah in pri več neodvisnih ponudnikih varnih sistemskih prostorov. Upravljanje kontinuitete poslovanja je opredeljeno v internem dokumentu Politika neprekinjenega poslovanja storitev Rekono. Oceno postopkov je izvedel neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje se redno ponavljata v skladu z ISO/IEC 27001.

2.12. Prenehanje delovanja ponudnika storitev

V primeru, če bo Rekono TSP prenehal z izvajanjem storitev zaupanja, bo o nameri prekinitve delovanja obvestil nacionalni nadzorni organ.

Poleg tega velja naslednje:

a) V primeru, če bo Rekono TSP prenehal z izvajanjem storitev zaupanja, bo izvedel vsaj sledeče:

- obvestil vse trenutne naročnike vsaj devetdeset (90) dni pred namenom prenehanja delovanja;

- uničil vse zasebne ključe, ki se uporabljajo v okviru storitve potrjevanja veljavnosti podpisov na način, da ključev ne bo možno povrniti oziroma ponovno uporabiti;
- ukinil avtorizacije dostopa vsem pogodbenim izvajalcem;
- če bo možno, prenesel naročniške pogodbe za izvajanje storitve na drugega ponudnika storitev zaupanja;

b) za razumen čas zagotovil objavo potrdil javnih ključev storitve ali prenesel obveznost na drugega ponudnika storitev.

2.13. Preverjanje skladnosti in ostale oblike nadzora

Zunanjo presojo delovanja po ISO/IEC 27001 in ISO/IEC 20000-1 izvaja neodvisni revizijski in certifikacijski organ. Ocenjevanje in certificiranje po ISO/IEC 27001 in ISO/IEC 20000-1 se izvajata enkrat letno.

Zunanje preverjanje skladnosti delovanja z Uredbo eIDAS izvaja organ za ugotavljanje skladnosti v skladu z veljavno zakonodajo.

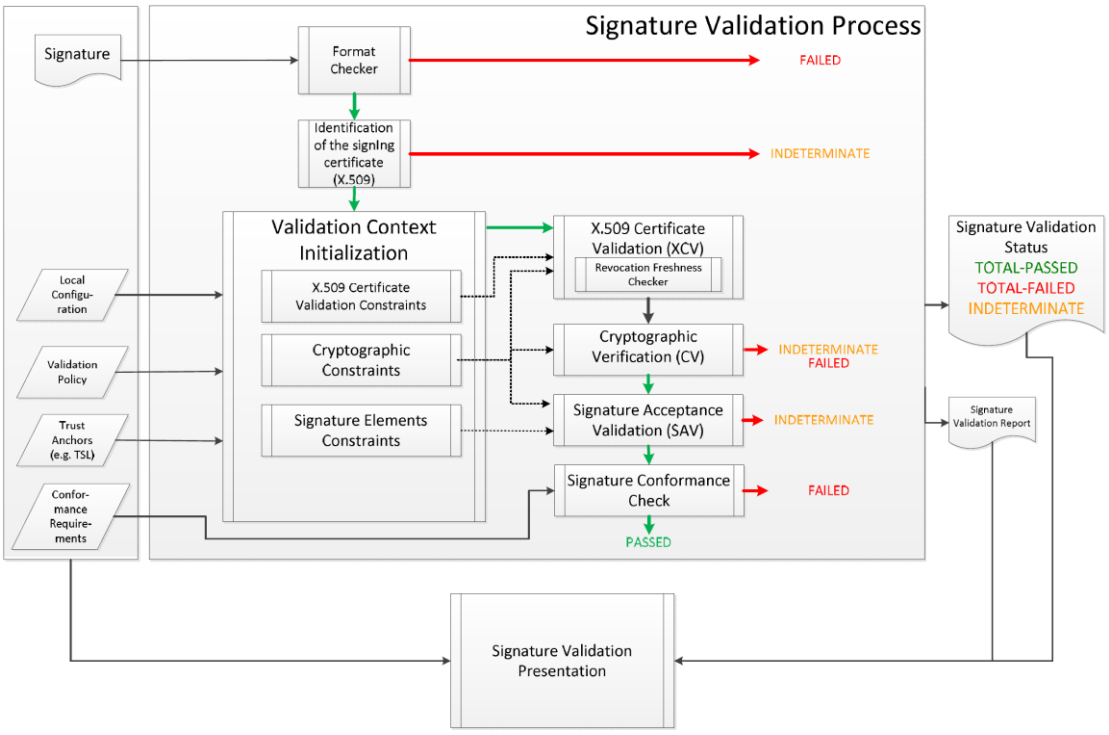
Poročilo presoje oziroma posamezni deli so lahko na voljo za vpogled vsaki strani, ki izrazi interes in dokaže, da je takšno razkritje potrebno. Oceno upravičenosti zahtevka za vpogled za vsak primer posebej izvede Rekono.PMA.

3. Tehnične lastnosti storitve potrjevanja veljavnosti podpisa

3.1. Postopek potrjevanja veljavnosti podpisa

Storitev Rekono QSVS izvaja potrjevanje veljavnosti podpisa v skladu z algoritmom za preverjanje veljavnosti podpisa, opredeljenem v ETSI EN 319 102-1. Potrjevanje veljavnosti kvalificiranih elektronskih podpisov/žigov (QESig/QESeal) in naprednih elektronskih podpisov/žigov, ki temeljijo na kvalificiranih potrdilih (AdES/QC), se izvaja v skladu s politiko potrjevanja podpisov na osnovi zaupanja vrednih seznamov ETSI TS 119 172-4 [22].

Na spodnji sliki, vzeti iz standarda ETSI EN 319 102-1, so predstavljene ključne lastnosti algoritma in gradniki, ki se uporabljajo za preverjanje veljavnosti podpisa.



Storitev Rekono QSVS podpira potrjevanje sledečih oblik elektronskih podpisov:

- PAdES, ETSI EN 319 142-1/-2
- XAdES, ETSI EN 319 132-1/-2
- CAdES, ETSI EN 319 122-1/-2

Storitev Rekono QSVS podpira potrjevanje zgoraj navedenih oblik elektronskih podpisov v skladu s politiko potrjevanja podpisov na osnovi zaupanja vrednih seznamov ETSI TS 119 172-4 [22].

3.2. Protokol potrjevanja veljavnosti podpisa

Storitev Rekono QSVS omogoča naročnikom posredovanje podpisanih podatkov preko aplikacijskega programskega vmesnika (API) ali preko spletnega grafičnega vmesnika. Preko vmesnika, ki je bil uporabljen za posredovanje zahtevka, bo tudi vrnjeno poročilo o potrditvi veljavnosti podpisa. V primeri posredovanja podatkov preko API je poročilo vrnjeno v obliki XML. V primeru posredovanja podatkov preko spletnega grafičnega vmesnika je poročilo vrnjeno v obliki PDF. V obeh primerih je poročilo o potrditvi veljavnosti podpisa ožigosano z naprednim elektronskim žigom storitve Rekono QSVS.

3.3. Vmesniki

3.3.1. Komunikacijski kanal

Storitev Rekono QSVS omogoča dostop do storitve in posredovanje podatkov preko protokola TLS. Dovoljeni sta različici TLSv1.2 in TLSv1.3.

V primeri posredovanja podatkov preko API se izvaja avtentikacija naročnika na osnovi digitalnega potrdila odjemalca.

V primeru posredovanja podatkov preko spletnega grafičnega vmesnika se mora naročnik identificirati z računom Rekono.

Storitev Rekono QSVS izvaja preverjanje statusa potrdil na osnovi CRL in OCSP, ter spletnih naslovov navedenih v potrdilih, ki se jih preverja.

3.3.2. Ponudnik storitve potrjevanja podpisov – ostali ponudniki storitev zaupanja

Storitev Rekono QSVS preverja status potrdil glede na CRL in OCSP, ki jih objavljajo ponudniki storitev zaupanja, ki so izdali dotično potrdilo. Preverjanje se izvaja v skladu z RFC 5280 [3], ter dodatno RFC 6960 [29] za OCSP. Objava in dostopnost CRL ter OCSP je odgovornost ponudnika storitev zaupanja, ki je izdal dotično potrdilo.

Status ponudnika storitev zaupanja, ki je izdal dotično potrdilo, se preverja na nacionalnih zanesljivih seznamih, ki se preverijo na osnovi seznama vseh seznamov (List of Trusted Lists – LOTL), ki ga objavlja Evropska komisija.

3.4. Poročilo o potrditvi veljavnosti podpisa

Poročilo o potrditvi veljavnosti podpisa vsebuje raven podpisa ter status preverjanja. Struktura poročila o potrditvi veljavnosti podpisa je povzeta po ETSI TS 119 102-2 [22].

Raven podpisa je lahko QESig, QESeal, AdESig-QC, AdESeal-QC ali QTSA:

- QESig, označuje kvalificirani elektronski podpis
- QESeal, označuje kvalificirani elektronski žig

- AdESig-QC, označuje napredni elektronski podpis, ki temelji na kvalificiranem potrdilu
- AdESeal-QC, označuje napredni elektronski žig, ki temelji na kvalificiranem potrdilu
- QTSA, označuje kvalificirani elektronski časovni žig

Oznaka status preverjanja je v skladu z ETSI TS 119 102-2 [21] in je ena od vrednosti:

- TOTAL-PASSED, ko so uspela kriptografska preverjanja podpisa (vključno s preverjanji zgoščenj posameznih podatkovnih objektov, ki so bili posredno podpisani) in uspešno opravljena vsa preverjanja, predpisana s politiko potrjevanja podpisov.
- TOTAL-FAILED, ko kriptografska preverjanja podpisa niso uspela (vključno s preverjanji zgoščenj posameznih podatkovnih objektov, ki so bili posredno podpisani), ali je ugotovljeno, da je bilo podpisno potrdilo v času generiranja podpisa neveljavno ali ker podpis ni skladen z enim od osnovnih kriptografskih standardov do te mere, da ga gradnik kriptografskega preverjanja ne more obdelati.
- INDETERMINATE, ko je rezultati opravljenih preverjanj nedoločen in ne omogoča ugotovitve podpisa TOTAL-PASSED ali TOTAL-FAILED.

Poročilo vsebuje tudi:

- dodatne podrejene oznake statusa preverjanja so v skladu z ETSI TS 119 102-1 [20];
- status preverjanja elektronskega časovnega žiga, če je bil dodan podatkom, ki so bili posredovani v preverjanje;
- datum in čas preverjanja v obliki UTC.
- podrobnosti dokumenta (stanje podpisov, ime dokumenta oziroma datoteke, zgoščeno vrednost SHA-256 dokumenta
- podrobnosti preverjanja posameznega podpisa

4. Dodatki

4.1. Reference

[1] RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

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

[3] RFC 5280 "Internet X.509 Public Key Infrastructure Certificates and Certificate Revocation List (CRL) Profile"

[4] RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"

[5] ETSI EN 319 401 "General Policy Requirements for Trust Service Providers"

[6] Uredba eIDAS "UREDBA (EU) št. 910/2014 EVROPSKEGA PARLAMENTA IN SVETA z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES"

[7] ETSI TR 119 001 "Definitions and abbreviations"

[8] ETSI EN 319 412 Part1: "Overview and common data structures"

[9] ETSI EN 319 412 Part2: "Certificate profile for certificates issued to natural persons"

[10] ETSI EN 319 412 Part3: "Certificate profile for certificates issued to legal persons"

[11] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 "on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market"

[12] ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps"

[13] Rekono TSP Pravila delovanja

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

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

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

[17] ETSI TS 119 312: "Electronic signatures and Infrastructures (ESI); Cryptographic Suites"

[18] List of Trusted Lists (https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml)

[19] Zanesljivi seznam (o ponudnikih kvalificiranih storitev zaupanja) (http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/eIDAS/SI_TL.xml)

[20] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"

[21] ETSI TS 119 102-2: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"

[22] ETSI TS 119 172-4: " Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists"

[23] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures"

[24] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles"

[25] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures"

[26] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures "

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

[28] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures"

[29] RFC6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"

[30] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services"