REKONO elektronske storitve zaupanja

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: 07.04.2026 12:59

REKONO elektronske storitve zaupanja

Ponudnik storitev zaupanja Rekono TSP; RekonoQSSAS Pravila delovanja (Practice Statement)

Kvalificirana storitev zaupanja za upravljanje oddaljenih kvalificiranih naprav za ustvarjanje elektronskega podpisa in elektronskega žiga

Različica:	1.0
Datum izdaje:	07. april 2026
Datum uveljavitve:	07. maj 2026

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:

Razl.	Datum	Opis / opomba
1.0	05.04.2026	Prva izdaja.

Kazalo

1. Uvod 5
1.1. Pregled 5
1.2. Identifikacija storitve in politike 6
1.3. Obseg storitve 6
1.4. Udeleženci 7
1.4.1. Ponudnik storitve SSAS (SSASP) 7
1.4.2. Naročniki in podpisniki 7
1.4.3. Tretje osebe 8
1.5. Upravljanje dokumenta 8
1.5.1. Organizacija, ki upravlja ta dokument 8
1.5.2. Postopek odobritve pravil delovanja 8
1.5.3. Objava 8
2. Objave in repozitorij 9
2.1. Repozitorij 9
2.2. Objavljene informacije 9
2.3. Čas in pogostost objav 9
2.4. Dostop do repozitorijev 9
3. Inicializacija podpisnih ključev uporabnikov storitve RekonoQSSAS 10
3.1. Tvorjenje podpisnih ključev 10
3.1.1. Model zunanjega shranjevanja ključev 10
3.1.2. Podpisni ključi 10
3.2. Povezovanje sredstev eID in identitete 11
3.2.1. Preverjanje istovetnosti 11
3.2.2. Avtentikacija na Rekono ID 11
3.3. Povezovanje potrdil 11
3.4. Zagotavljanje sredstev eID 11
4. Življenjski cikel podpisnih ključev 12
4.1. Aktivacija podpisa 12
4.2. Dodatni elementi ob aktivaciji in ustvarjanju podpisa 12
4.2.1. Časovna omejitev seje 12
4.2.2. Privolitev podpisnika 12
4.2.3. 4.1.5 Preverjanje veljavnosti potrdila 12
4.3. Brisanje podpisnih ključev 12
4.4. Varnostno kopiranje in obnovitev podpisnih ključev 13
5. Upravljanje objektov, osebja in operativni nadzor 14
5.1. Splošno 14
5.2. Fizično varovanje 14
5.3. Organizacijski varnostni ukrep 14

5.4. Zahteve za osebje ... 14
5.5. Postopki zbiranja in upravljanja revizijskih sledi ... 14
5.6. Arhiviranje zapisov ... 14
5.7. Postopki ob ogroženosti in okrevalni načrt ... 14
5.7.1. Postopki za odzivanje na varnostne incidente in nepravilnosti ... 14
5.7.2. Okrevalni načrt v primeru naravne ali druge nesreče ... 15
5.8. Prenehanje storitve ... 15
6. Tehnične varnostne kontrole ... 16
6.1. Varnostne kontrole računalnikov ... 16
6.2. Tehnični nadzor življenjskega cikla ... 16
6.3. Varnostne kontrole na ravni računalniškega omrežja ... 16
6.4. Kriptografske kontrole ... 16
7. QSCD - Certifikacija in konfiguracija ... 17
7.1. Sestava QSCD ... 17
7.2. Operativna konfiguracija QSCD ... 17
7.3. Vloge in nadzor dostopa v SAM ... 17
7.4. Kartice operaterjev in kvorum ... 18
7.5. Infrastrukturni ključi SAM ... 18
7.6. Revizijsko beleženje SAM ... 18
8. Upravljanje podatkov za aktivacijo podpisa ... 19
8.1. SAD ... 19
8.2. SAD pri neposrednem povezovanju identitete ... 19
9. Ostale poslovne in pravne zadeve ... 20
10. Reference ... 21
10.1. Normativne reference ... 21
10.2. Regulativne reference ... 21
10.3. Informativne reference ... 22
11. Priloga - Modeli namestitve SCA ... 23
11.1. Pregled ... 23
11.2. Zunanja SCA ... 23
11.3. Rekono SCA ... 23
12. Priloga - Definicije in okrajšave ... 24
12.1. Definicije ... 24
12.2. Okrajšave ... 25

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 upravljanje oddaljenih kvalificiranih naprav za ustvarjanje elektronskega podpisa in elektronskega žiga (v nadaljevanju storitev RekonoQSSAS) in druge storitve zaupanja, kot so overjanje digitalnih potrdil za kvalificirani elektronski podpis, kvalificirani elektronski žig, napredni elektronski podpis, napredni elektronski žig, elektronsko avtentikacijo, izdajanje kvalificiranih elektronskih časovnih žigov, kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih podpisov ter kvalificirano storitev potrjevanja veljavnosti kvalificiranih elektronskih žigov.

Pričujoči dokument je RekonoQSSAS Pravila delovanja kvalificirane storitve zaupanja RekonoQSSAS. Storitev RekonoQSSAS izvaja in upravlja Rekono d.o.o. kot kvalificirano storitev zaupanja za upravljanje oddaljenih kvalificiranih naprav za ustvarjanje elektronskega podpisa in elektronskega žiga. Vsebuje pogoje uporabe in opis pravil ter postopkov, ki jih izvaja Rekono d.o.o. za izvajanje kvalificirane storitve upravljanja oddaljenih naprav za ustvarjanje elektronskega podpisa in elektronskega žiga. RekonoQSSAS 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.

Rekono d.o.o. izvaja storitev RekonoQSSAS v skladu z Uredbo (EU) št. 910/2014, spremenjeno z Uredbo (EU) 2024/1183 ter EN 319 421 V1.3.1, EN 319 422 V1.1.1 in EN 391 401.

Storitev RekonoQSSAS zagotavlja storitev za strežniško podpisovanje (SSAS) v skladu z ETSI TS 119 431-1 V1.3.1 (2024-12), Priloga A (politika EUSPv2). Storitev upravlja življenjski cikel podpisnih ključev v imenu podpisnikov in ustvarjalcev žigov. Zagotavlja, da se podpisni ključi tvorijo, aktivirajo in uporabljajo izključno znotraj certificirane naprave QSCD pod izključnim nadzorom podpisnika (za podpise) oziroma pod nadzorom ustvarjalca žiga (za žige).

Storitev uporablja SAM (Signature Activation Module) in strojni varnostni modul (HSM) kot oddaljeno napravo QSCD. SAM je certificiran v skladu s profilom zaščite EN 419241-2 (EAL4+AVA_VAN.5). HSM je certificiran v skladu z EN 419221-5.

1.2. Identifikacija storitve in politike

Za to storitev veljajo sledeči identifikatorji:

Atribut	Vrednost
Ime storitve	RekonoQSSAS
Ponudnik storitve	Rekono d.o.o.
Politika SSAS	EUSPv2 — EU SSAS Policy
OID politike	0.4.0.19431.1.1.4
Regulativna podlaga	Uredba (EU) št. 910/2014, spremenjena z Uredbo (EU) 2024/1183, člena 29a in 39a
Izvedbena uredba	Izvedbena uredba Komisije (EU) 2025/1567
Referenčni standard	ETSI TS 119 431-1 V1.3.1 (2024-12), Priloga A (EUSPv2)
QSCD	SAM + HSM

1.3. Obseg storitve

Storitev RekonoQSSAS pokriva sledeči kvalificirani storitvi zaupanja:

- Kvalificirana storitev zaupanja za upravljanje oddaljenih kvalificiranih naprav za ustvarjanje elektronskega podpisa (člen 29a Uredbe (EU) št. 910/2014).
- Kvalificirana storitev zaupanja za upravljanje oddaljenih kvalificiranih naprav za ustvarjanje elektronskega žiga (člen 39a Uredbe (EU) št. 910/2014, smiselna uporaba).

Storitev RekonoQSSAS vključuje sledeče komponente, kot jih določa ETSI TS 119 431-1:

- Storitev tvorjenja podpisnih ključev: Tvori podpisne ključe znotraj QSCD.
- Storitev povezovanja potrdil: Poveže potrdila, izdana s strani Rekono CA, z ustreznimi podpisnimi ključi.
- Storitev povezovanja sredstev eID / identitete: Poveže avtentikacijo podpisnika (prek Rekono ID) z ustreznimi podpisnimi ključi.
- Storitev aktivacije podpisa: Preveri SAD in aktivira podpisne ključe za ustvarjanje podpisa.
- Storitev brisanja podpisnih ključev: Uniči podpisne ključe, ko je to potrebno.
- Storitev zagotavljanja sredstev eID (opcijsko): Zagotavlja sredstva eID podpisnikom prek Rekono ID.

Storitev RekonoQSSAS podpira dva modela namestitve aplikacije za ustvarjanje podpisa (SCA):

- Zunanja SCA: Zunanja stranka upravlja lastno SCA. Pošlje pred računano vrednost DTBS/R na vmesnik RekonoQSSAS in prejme surovo vrednost podpisa.
- Rekono SCA: Stranka pošlje dokument na vmesnik Rekono SCA. SCA izračuna DTBS/R, orkestrira podpisovanje prek SSA in vrne podpisan dokument.

SCA je dodatna storitvena plast nad SSA. Ocena skladnosti za SSAS (EUSPv2) je neodvisna od modela namestitve SCA.

1.4. Udeleženci

1.4.1. Ponudnik storitve SSAS (SSASP)

Storitev RekonoQSSAS upravlja:

Atribut	Vrednost
Organizacija	Rekono d.o.o.
Naslov	Ukmarjeva ulica 2, Ljubljana, Slovenija
E-pošta	info@rekono.si
Spletna stran	https://www.rekono.si
ID za DDV	SI60762802

Rekono d.o.o. je kvalificirani ponudnik storitev zaupanja, vpisan na zaupanja vreden seznam EU. Rekono d.o.o. nosi celotno odgovornost za storitev, vključno z deli, ki so preneseni na zunanje izvajalce.

Organizacijska struktura temelji na treh enotah:

- RekonoPMA (Policy Management Authority): Upravlja politike, pravila delovanja in nadzor skladnosti.
- RekonoOA (Operations Authority): Upravlja vsakodnevno delovanje, upravljanje ključev, infrastrukturo in odzivanje na incidente.
- RekonoRA (Registration Authority): Upravlja preverjanje istovetnosti, registracijo naročnikov in vpis.

1.4.2. Naročniki in podpisniki

V okviru storitve RekonoQSSAS je podpisnik ali ustvarjalec žiga lahko:

- Fizična oseba (za kvalificirane elektronske podpise).
- Fizična oseba, identificirana v povezavi s pravno osebo (za kvalificirane elektronske podpise).
- Pravna oseba (za kvalificirane *elektronske* žige).

Razmerje med podpisnikom/ustvarjalcem žiga in naročnikom je skladno z ETSI EN 319 411-1, člen 5.4.2.

1.4.3. Tretje osebe

Tretje osebe so subjekti, ki se zanašajo na kvalificirane elektronske podpise ali žige, ustvarjene s storitvijo RekonoQSSAS. Tretje osebe morajo pred sprejemom elektronsko podpisanega dokumenta preveriti veljavnost in status potrdil.

1.5. Upravljanje dokumenta

1.5.1. Organizacija, ki upravlja ta dokument

Ta dokument upravlja Rekono d.o.o..

1.5.2. Postopek odobritve pravil delovanja

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..

1.5.3. Objava

Pravila delovanja so objavljena na javni spletni strani Rekono TSP na naslovu https://www.rekono.si. Dostopna so 24 ur na dan, 7 dni v tednu. V primeru izpada sistema Rekono d.o.o. uporabi vse razumne ukrepe za vzpostavitev dostopnosti.

2. Objave in repozitorij

2.1. Repozitorij

Rekono TSP uporablja notranje in javne repozitorije.

Javni repozitoriji so dostopni na sledečih spletnih naslovih:

Javne spletne strani:	https://www.rekono.si http://pki.rekono.si/cps/

2.2. Objavljene informacije

Rekono TSP objavlja sledeče informacije:

- Pravila delovanja RekonoQSSAS (trenutno verzijo in zgodovino verzij).
- Splošne pogoje za naročnike in tretje osebe.
- Sezname preklicanih digitalnih potrdil (CRL), ki jih izdajajo overitelji Rekono TSP.
- Naslove storitev OCSP za preverjanje statusa potrdil.
- Digitalna potrdila overiteljev za vse verige zaupanja, ki jih uporablja storitev RekonoQSSAS.

2.3. Čas in pogostost objav

Seznami preklicanih potrdil se objavljajo v skladu z urnikom, določenim v Rekono TSP Pravilih delovanja. Vse ostale informacije se objavijo ob spremembi ali takoj, ko postanejo dostopne.

2.4. Dostop do repozitorijev

V javnih repozitorijih so objavljene samo javne informacije, ki so dostopne samo za branje. Repozitoriji imajo vzpostavljene ustrezne tehnične varnostne mehanizme za zaščito pred nepooblaščenimi spremembami podatkov ter mehanizme za zagotavljanje razpoložljivosti podatkov.

3. Inicializacija podpisnih ključev uporabnikov storitve RekonoQSSAS

3.1. Tvorjenje podpisnih ključev

Podpisni ključi se tvorijo znotraj naprave QSCD. QSCD sestavljata SAM in strojni varnostni modul (HSM). HSM izvede kriptografsko tvorjenje para ključev. QSCD (SAM + HSM) deluje v certificirani konfiguraciji.

Veljajo sledeče zahteve iz EN 419241-1:

- Podpisni ključi se tvorijo in uporabljajo v okolju, zaščitenem pred posegi.
- Kriptografski algoritmi in dolžine ključev so skladni z dogovorjenimi kriptografskimi mehanizmi ENISA.
- Podpisni ključi so zaščiteni z infrastrukturnim ključem v HSM.
- Inicializacija naprave je izvedena skladno s smernicami iz certifikacijske dokumentacije SAM.
- Parametri algoritma se nastavijo ob tvorjenju ključa.
- Čas tvorjenja ključa se zabeleži v revizijski dnevnik.

3.1.1. Model zunanjega shranjevanja ključev

HSM ne hrani trajno vseh podpisnih ključev uporabnikov. Po tvorjenju ključa SAM vrne šifriran blob ključa. Zasebni ključ znotraj bloba je šifriran z infrastrukturnim ključem v HSM. Blob se shrani v podatkovni bazi ključev SSA.

Ob vsakem postopku podpisovanja SSA pridobi blob iz podatkovne baze in ga posreduje SAM-u. SAM naloži ključ v HSM za čas operacije. Po podpisu se ključ odstrani iz HSM.

Ta model je skladen z EN 419241-1, člen 5.13.3.1. Blob ključa je zaščiten z infrastrukturnim ključem v HSM in ga ni mogoče uporabiti zunaj QSCD.

3.1.2. Podpisni ključi

Storitev RekonoQSSAS podpira enkratne podpisne ključe za elektronske podpise in dolgotrajne ključe za večkratno uporabo.

Enkratni podpisni ključ je vezan na natanko eno sejo podpisovanja. Ključ se tvori, uporabi in izbriše znotraj ene seje. Pri enkratnih ključih se ključ poveže bodisi s sredstvom eID bodisi neposredno z identiteto.

Dolgotrajni podpisni ključ se lahko uporabi za več podpisov v več sejah. Pri dolgotrajnih ključih se ključ poveže s sredstvom eID.

3.2. Povezovanje sredstev eID in identitete

Podpisni ključ se poveže bodisi s sredstvom eID (za dolgotrajne ključe ali enkratne podpisne ključe) bodisi neposredno z identiteto (za enkratne podpisne ključe). Veljajo sledeče zahteve.

3.2.1. Preverjanje istovetnosti

Vloga in registracija podpisnika se izvaja v skladu z Rekono TSP Pravili delovanja.

Za fizične osebe preverjanje istovetnosti ustreza srednji ali visoki ravni zanesljivosti.

Za pravne osebe preverjanje istovetnosti ustreza srednji ali visoki ravni zanesljivosti.

3.2.2. Avtentikacija na Rekono ID

Postopek avtentikacije je prenesen na Rekono ID, ki je ponudnik identitete (IdP) v upravljanju Rekono d.o.o. Rekono ID izdaja sredstva eID na ravneh zanesljivosti srednja (substantial) in visoka (high).

Ob prenosu avtentikacije na Rekono ID:

- Rekono ID izpolnjuje zadevne zahteve Izvedbene uredbe Komisije (EU) 2015/1502.
- Značilnosti in zasnova sredstva eID ustrezajo srednji ali visoki ravni zanesljivosti.
- Mehanizem avtentikacije ustreza srednji ali viski ravni zanesljivosti.

Podatki za identifikacijo osebe, povezani z referenco sredstva eID, so enaki podatkom, povezanim s subjektom v pripadajočem potrdilu.

Rekono kot SSASP ščiti celovitost povezave med podpisnim ključem in referenco sredstva eID oziroma identiteto uporabnika.

3.3. Povezovanje potrdil

Potrdila, ki jih izda Rekono TSP CA, se povežejo z ustreznimi podpisnimi ključi znotraj SSAS. Velja sledeče:

- Potrdilo se poveže s podpisnim ključem.
- Povezava potrdila se preveri.
- Celovitost povezav med ključi in potrdili je zaščitena.

3.4. Zagotavljanje sredstev eID

Sredstva eID podpisnikom zagotavlja Rekono ID. Sredstva eID ustvarjalcem žigov zagotavlja Rekono ID ali Rekono TSP.

4. Življenjski cikel podpisnih ključev

4.1. Aktivacija podpisa

Storitev aktivacije podpisa preveri SAD in aktivira podpisni ključ za ustvarjanje vrednosti digitalnega podpisa. Velja sledeče:

- Avtentikacija podpisnika je zahtevana pred aktivacijo podpisnega ključa.
- Nadzor dostopa preprečuje nepooblaščeno uporabo podpisnih ključev.
- Aktivacija podpisnega ključa sledi zahtevam za izključni nadzor.
- Podpisni ključi se uporabljajo v QSCD.
- QSCD deluje v certificirani konfiguraciji.
- SAM je certificiran v skladu z EN 419241-2.

4.2. Dodatni elementi ob aktivaciji in ustvarjanju podpisa

4.2.1. Časovna omejitev seje

Kadar je avtentikacija neposredno povezana z identiteto (enkratni podpisni ključi), se seja podpisovanja zaključi najkasneje 30 minut po končanem preverjanju istovetnosti.

4.2.2. Privolitev podpisnika

Podpisni ključi se lahko uporabijo samo v primerih, za katere je podpisnik ali ustvarjalec žiga dal privolitev. Za elektronske podpise povezane neposredno z identiteto RekonoSSAS zagotavlja, da podpisnik z izrecnim dejanjem potrdi strinjanje s podatki, ki jih podpisuje.

4.2.3. 4.1.5 Preverjanje veljavnosti potrdila

RekonoQSSAS pred uporabo dolgotrajnega podpisnega ključa preveri, da je pripadajoče digitalno potrdilo veljavno (ni preteklo, ni preklicano).

4.3. Brisanje podpisnih ključev

Podpisni ključi se uničijo v sledečih primerih:

- Ob preklicu pripadajočega potrdila.
- Na zahtevo podpisnika ali ustvarjalca žiga.
- Ob koncu seje podpisovanja pri enkratnih podpisnih ključih.

Brisanje ključa se izvede z odstranitvijo bloba ključa iz podatkovne baze SSA. Po brisanju ključa ni mogoče rekonstruirati.

4.4. Varnostno kopiranje in obnovitev podpisnih ključev

Za varnostno kopiranje ključev velja sledeče:

- Število podvojenih naborov podatkov ne presega minimuma, potrebnega za zagotavljanje neprekinjenosti storitve.
- Varnost varnostnih kopij je na enaki ravni kot varnost izvirnih naborov podatkov.

5. Upravljanje objektov, osebja in operativni nadzor

5.1. Splošno

5.2. 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.

5.3. Organizacijski varnostni ukrep

Organizacijski varnostni ukrepi se izvajajo kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 5.2.

5.4. Zahteve za osebje

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 5.3.

5.5. Postopki zbiranja in upravljanja revizijskih sledi

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 5.4.

Dodatno, SAM tvori revizijske zapise zaščitene s HMAC. Celovitost se preverja z infrastrukturnimi ključi zaščitenimi s HSM.

5.6. Arhiviranje zapisov

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 5.5.

5.7. Postopki ob ogroženosti in okrevalni načrt

5.7.1. Postopki za odzivanje na varnostne incidente in nepravilnosti

Overitelj 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.

5.7.2. Okrevalni načrt v primeru naravne ali druge nesreče

V primeru naravne ali druge nesreče, pri kateri zasebni ključi niso bili uničeni, bodo storitve vzpostavljene nazaj v najkrajšem možnem času. Postopki so podrobneje opredeljeni v zaupnem delu notranjih pravil delovanja ponudnika storitev zaupanja Rekono TSP.

5.8. Prenehanje storitve

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 5.8.

6. Tehnične varnostne kontrole

6.1. Varnostne kontrole računalnikov

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 6.5.

6.2. Tehnični nadzor življenjskega cikla

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 6.6.

6.3. Varnostne kontrole na ravni računalniškega omrežja

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 6.7.

6.4. Kriptografske kontrole

Storitev RekonoQSSAS uporablja kriptografske algoritme, skladne z dogovorjenimi kriptografskimi mehanizmi (Agreed Cryptographic Mechanisms [7]).

V storitvi RekonoQSSAS se uporabljajo sledeči kriptografski algoritmi:

Funkcija	Algoritem	Dolžina ključa
Tvorjenje podpisnih ključev	RSA / ECDSA	RSA 3072+ / ECC P-256+
Ustvarjanje digitalnega podpisa	RSA-SHA256, RSA-SHA384, RSA-SHA512, ECDSA	Po vrsti ključa
Infrastrukturni ključi SAM	RSA	3072 ali 4096
HMAC (celovitost dnevnikov)	SHA-256, SHA-384, SHA-512	256, 384 ali 512 bitov
AES (izvoz zasebne konfiguracije)	AES	128, 192 ali 256 bitov

7. QSCD - Certifikacija in konfiguracija

7.1. Sestava QSCD

QSCD, ki ga uporablja RekonoQSSAS, sestavljata:

Komponenta	Certifikacija
Modul za aktivacijo podpisa (SAM)	Common Criteria EAL4+AVA_VAN.5 po profilu zaščite EN 419241-2
Kriptografski modul (HSM)	Common Criteria certificiran po EN 419221-5

Storitev RekonoQSSAS izpolnjuje zahteve, določene v certifikacijskem poročilu QSCD.

7.2. Operativna konfiguracija QSCD

QSCD deluje v konfiguraciji, kot je opisana v certifikacijski dokumentaciji. To vključuje:

- Naprava SAM deluje na utrjenem operacijskem sistemu.
- Izvršljiva datoteka SAM in orodje za administracijo sta edini nameščeni aplikaciji.
- Različica programske opreme HSM se vzdržuje na certificirani različici.

7.3. Vloge in nadzor dostopa v SAM

SAM uveljavlja sledeče vloge:

Vloga	Odgovornost
Prvi privilegiran uporabnik (FPU)	Imetnik kartic FPU. Potreben (skupaj z OPU) za ustvarjanje, inicializacijo in obnovitev zasebne konfiguracije SAM. Potreben za vzpostavitev statične konfiguracije.
Operativni privilegiran uporabnik (OPU)	Imetnik kartic OPU. Potreben za zagon SAM, zamenjavo dinamične konfiguracije in preverjanje revizijskih zapisov.
Konfiguracijski privilegiran uporabnik	Podpisuje dinamično konfiguracijo. Določa prepoznane podpisne storitve in avtorizacijske strežnike.
Privilegiran uporabnik podpisne storitve	Komponenta SSA. Kliče storitvene funkcije SAM (tvorjenje ključev, podpisovanje, upravljanje ključev).
Podpisnik	Lastnik podpisnih ključev. Ne kliče funkcij SAM neposredno. Avtorizacija prek avtorizacijskega strežnika.

Vloga	Odgovornost
Avtorizacijski strežnik	Tvori elemente SAD, ki jih SAM zaupa.
Administrator kartic	Imetnik kartic. Potreben samo za operacije zamenjave kartic FPU in OPU.

7.4. Kartice operaterjev in kvorum

Kriptografski ključi SAM so zaščiteni z dvema naboroma kartic operaterjev :

- Prvi privilegiran uporabnik: Zaščiti del zasebne konfiguracije in njeno varnostno kopijo. Kvorum 2 ali več (N od M, N ≥ 2).
- Operativni privilegiran uporabnik: Zaščiti del zasebne konfiguracije in njeno varnostno kopijo. Potreben za zagon SAM. Kvorum 1 (1/M).

7.5. Infrastrukturni ključi SAM

Zasebna konfiguracija SAM vsebuje sledeče infrastrukturne ključe:

Ključ	Zaščita	Namen
Authentication	OPU	Avtentikacija Operativnega privilegiranega uporabnika do SAM.
TLS server	OPU	Zasebni ključ TLS strežnika. Potrdilo se posreduje vsem entitetam podpisne storitve.
Key pair protection	OPU	Potreben za uporabo podpisnih ključev v HSM. Vključen v ACL vseh podpisnih ključev.
Log signing (opu)	OPU	HMAC ključ za celovitost operativnih revizijskih zapisov.
Log signing (fpu)	FPU	HMAC ključ za celovitost administrativnih revizijskih zapisov.
Signer signing	OPU	RSA ključ za podpisovanje objektov podpisnih ključev in informacij o podpisnikih.

7.6. Revizijsko beleženje SAM

SAM tvori revizijske zapise za vse operacije. Vsak zapis je zaščiten s HMAC z ustreznim infrastrukturnim ključem. Zapisi vsebujejo časovne oznake, podrobnosti operacij in kode rezultatov.

Revizijski zapisi se preverjajo z administrativnim orodjem. Zahtevana je avtentikacija Operativnega privilegiranega uporabnika.

8. Upravljanje podatkov za aktivacijo podpisa

8.1. SAD

SAD poveže tri elemente: avtentikacijo podpisnika, identifikator podpisnega ključa in DTBS/R. SAD tvori avtorizacijski strežnik, ki SAD podpiše z ključem, ki mu SAM zaupa.

8.2. SAD pri neposrednem povezovanju identitete

Kadar je avtentikacija neposredno povezana z identiteto:

- SAD vsebuje enolični identifikator seje podpisovanja, enolično povezan s SSAS.
- SAD vsebuje enolični identifikator postopka preverjanja istovetnosti.

9. Ostale poslovne in pravne zadeve

Kot je navedeno v Pravilih delovanja Rekono TSP, poglavje 9.

10. Reference

10.1. Normativne reference

[1] ETSI EN 319 401 V3.1.1 (2024-06): General Policy Requirements for Trust Service Providers.

[2] ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[3] EN 419241-1: Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements.

[4] EN 419241-2: Trustworthy Systems Supporting Server Signing — Part 2: Protection Profile for QSCD for Server Signing.

[5] EN 419221-5: Protection Profiles for TSP Cryptographic Modules — Part 5: Cryptographic Module for Trust Services.

[6] ETSI TS 119 461: Policy and security requirements for trust service components for identity proofing of trust service subjects.

[7] ENISA: Agreed Cryptographic Mechanisms (European Cybersecurity Certification Group, Sub-group on Cryptography).

[8] ETSI TS 119 431-1 V1.3.1 (2024-12): Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.

[9] ETSI TS 119 431-2: Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.

[10] ETSI EN 319 403: Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.

10.2. Regulativne reference

[11] Uredba (EU) št. 910/2014 (Uredba eIDAS).

[12] Uredba (EU) 2024/1183 o spremembi Uredbe (EU) št. 910/2014 (eIDAS 2.0).

[13] Izvedbena uredba Komisije (EU) 2025/1567 z dne 29. julija 2025 o upravljanju oddaljenih naprav QSCD kot kvalificiranih storitev zaupanja.

[14] Uredba (EU) 2016/679 (Splošna uredba o varstvu podatkov — GDPR).

[15] Zakon o elektronski identifikaciji in storitvah zaupanja (ZEISZ), Uradni list RS, št. 121/21.

[16] Zakon o varstvu osebnih podatkov, Uradni list RS, št. 163/22.

[17] Izvedbena uredba Komisije (EU) 2015/1502 z dne 8. septembra 2015 o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu.

10.3. Informativne reference

[1] ETSI TS 119 432: Protocols for remote digital signature creation.

[2] ETSI EN 319 122: CAdES digital signatures.

[3] ETSI EN 319 132: XAdES digital signatures.

[4] ETSI EN 319 142: PAdES digital signatures.

[5] ETSI EN 319 182: JAdES digital signatures.

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

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

[8] Ponudnik storitev zaupanja Rekono TSP Pravila delovanja, 1.7.2

11. Priloga - Modeli namestitve SCA

11.1. Pregled

Aplikacija za ustvarjanje podpisa (SCA) je komponenta, ki upravlja dokument za podpis, izračuna DTBS/R in vgradi vrednost podpisa v podpisan dokument. SCA je opredeljena v EN 419241-1, člen 5.13. SCA deluje nad SSAS in ni del QSCD.

Storitev RekonoQSSAS podpira dva modela namestitve SCA.

11.2. Zunanja SCA

V tem modelu zunanja stranka upravlja lastno SCA. Potek:

- SCA zunanje stranke izračuna DTBS/R iz dokumenta za podpis.
- SCA pošlje DTBS/R na vmesnik RekonoQSSAS (SSA).
- SSA orkestrira avtentikacijo podpisnika (prek Rekono ID) in aktivacijo podpisa (prek SAM).
- SSA vrne surovo vrednost digitalnega podpisa SCA.
- SCA vgradi vrednost podpisa v podpisan dokument.

V tem modelu Rekono zagotavlja samo SSAS (SSA + QSCD). Zunanja stranka je odgovorna za oblikovanje podpisa (PAdES, XAdES, CAdES, JAdES) in celovitost dokumenta.

11.3. Rekono SCA

V tem modelu Rekono d.o.o. upravlja SCA. Potek:

- Stranka pošlje dokument (PDF, XML ipd.) na vmesnik Rekono SCA.
- SCA izračuna DTBS/R.
- SCA prek SSA orkestrira avtentikacijo in podpisovanje.
- SCA vgradi vrednost podpisa v dokument.
- SCA vrne v celoti podpisan dokument stranki.

Rekono SCA podpira sledeče oblike in ravni podpisa:

- PAdES (PDF Advanced Electronic Signatures).
- XAdES (XML Advanced Electronic Signatures).
- CAdES (CMS Advanced Electronic Signatures).
- JAdES (JSON Advanced Electronic Signatures).

12. Priloga - Definicije in okrajšave

12.1. Definicije

Izraz	Definicija
Vrednost digitalnega podpisa	Rezultat kriptografske pretvorbe podatkovne enote, ki dokazuje njen izvor in celovitost.
DTBS/R	Data To Be Signed / Representation. Zgostitev ali reprezentacija dokumenta, predloženega v podpis.
Sredstvo eID	Materialna ali nematerialna enota, ki vsebuje podatke za identifikacijo osebe in se uporablja za avtentikacijo.
Referenca sredstva eID	Podatki v SSAS kot referenca na sredstvo eID za avtentikacijo podpisnika.
Enkratni podpisni ključ	Podpisni ključ, ki se tvori, certificira, uporabi in uniči na podlagi ene avtorizacije.
QSCD	Kvalificirana naprava za ustvarjanje elektronskega podpisa/žiga po Uredbi (EU) št. 910/2014.
Oddaljena naprava QSCD	QSCD, ki ga na daljavo upravlja QTSP v imenu podpisnika ali ustvarjalca žiga.
SAD	Signature Activation Data. Podatki, ki povežejo avtentikacijo podpisnika, podpisni ključ in DTBS/R.
SAM	Signature Activation Module. Komponenta, ki preveri SAD in aktivira podpisne ključe.
SAP	Signature Activation Protocol. Protokol za prenos SAD med podpisnikom in SAM.
SCA	Signature Creation Application. Komponenta, ki upravlja dokumente in oblike podpisa.
SCDev	Signature Creation Device. Naprava za ustvarjanje podpisa.
SSAS	Server Signing Application Service. Storitev aplikacije za strežniško podpisovanje.
SSASP	Server Signing Application Service Provider. Ponudnik storitve SSAS.
TW4S	Trustworthy System Supporting Server Signing. Zaupanja vreden sistem za strežniško podpisovanje.

12.2. Okrajšave

Okrajšava	Pomen
AES	Advanced Encryption Standard
CA	Certificate Authority — overitelj
CAdES	CMS Advanced Electronic Signatures
CRL	Certificate Revocation List — seznam preklicanih potrdil
ECDSA	Elliptic Curve Digital Signature Algorithm
ENISA	Agencija Evropske unije za kibernetsko varnost
EUSPv2	EU SSAS Policy (različica 2)
FPU	First Privileged User — prvoprivilegirani uporabnik
GDPR	General Data Protection Regulation — Splošna uredba o varstvu podatkov
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module — strojni varnostni modul
JAdES	JSON Advanced Electronic Signatures
JWS	JSON Web Signature
LoA	Level of Assurance — raven zanesljivosti
LoIP	Level of Identity Proofing — raven preverjanja istovetnosti
LSP	Lightweight SSAS Policy
mTLS	Mutual TLS — vzajemni TLS
NIS2	Direktiva (EU) 2022/2555 o kibernetski varnosti
NSP	Normalized SSAS Policy
OCSP	Online Certificate Status Protocol
OID	Object Identifier — identifikacijska oznaka objekta
OPU	Operation Privileged User — operativni privilegirani uporabnik
PAdES	PDF Advanced Electronic Signatures
PoP	Proof of Possession — dokaz posedovanja
QTSP	Qualified Trust Service Provider — kvalificirani ponudnik storitev zaupanja

Okrajšava	Pomen
RSA	Rivest–Shamir–Adleman
SSPU	Signing Service Privileged User — privilegirani uporabnik podpisne storitve
TLS	Transport Layer Security
XAdES	XML Advanced Electronic Signatures
ZEISZ	Zakon o elektronski identifikaciji in storitvah zaupanja