MitSoft

Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas

Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai

QTSP/PS-LT

Versija 1.00

Galioja nuo 2024-10-01

UAB „MIT-SOFT“, Kalvarijų g. 276-100, LT-08316 Vilnius, Tel. +370 233 3922, Faksas +370 5 213 6191, www.mitsoft.lt, info@mitsoft.lt, Įmonės kodas 120792080, PVM mokėtojo kodas LT207920811

Patvirtinimai

Versijų istorija

Versija	Galioja nuo	Aprašas
1.00	2024-10-01	Pirma oficiali dokumento versija

Dokumento patvirtinimas

	Vardas Pavardė	Data	Parašas
Peržiūrėjo	Adomas Birštunas	2024-08-13	
Patvirtino	Antanas Mitašiūnas	2024-08-20	

Turinys

1. ĮVADAS

Uždaroji akcinė bendrovė "MIT-SOFT" (toliau – MitSoft) įsteigta 1991 m. rugpjūčio 1 d. ir nuo 1996 m. dirba elektroninių dokumentų, turinčių tokią pat teisinę galią kaip ranka pasirašyti dokumentai popieriuje, sudarymo ir tikrinimo programinės įrangos kūrimo ir paslaugų teikimo srityje. Informacija apie MitSoft yra pateikiama interneto svetainėje http://www.mitsoft.lt/.

MitSoft veiklos nuostatus suskirstė į tris dalis:

- Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai (QTS PS) aprašo visoms kvalifikuotoms paslaugoms bendras praktikas;
- Ilgalaikės apsaugos paslaugų veiklos nuostatai (QLPS PS) ir Laiko žymų paslaugų veikos nuostatai (QTSS PS) aprašo praktikas specifines kiekvienai kvalifikuotai paslaugai.

1.1. Apžvalga

Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai (QTS PS) remiasi šiais teisės aktais ir norminiais dokumentais:

a) Europos Parlamento ir Tarybos Reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB [eIDAS];

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

Pastaba dėl sutrumpinimų apibrėžimų. Viskas, kas yra sakoma šiame dokumente, taikoma tik MitSoft QTSP.

Aktuali QTS PS versija yra prieinama MitSoft interneto svetainėje.

1.2. Kontaktiniai duomenys

Veiklos nuostatus prižiūri uždaroji akcinė bendrovė "MIT-SOFT", kurios kontaktiniai duomenys yra pateikti 2 lentelėje.

2 lentelė. MitSoft QTSP kontaktiniai duomenys

QTSP:	Uždaroji akcinė bendrovė "MIT-SOFT"
Adresas:	Kalvarijų g. 276-100, LT-08316 Vilnius
Tel:	+370 5 233 3922
URL:	https://www.mitsoft.lt/
El. paštas:	info@mitsoft.lt

2. Nuorodos

[eIDAS] – Europos Parlamento ir Tarybos Reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.

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

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

[ISO 27002] – ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security management systems - Requirements".

[ISO 27005] – ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection – Guidance on managing security risks".

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

[RFC 5816] – RFC 5816 ESSCertIDv2 Update for RFC 3161.

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

3. Sąvokų ir santrumpų apibrėžimas

Abonentas: juridinis ar fizinis asmuo, turintis sutartinius abonento įsipareigojimus su kvalifikuotų patikimumo užtikrinimo paslaugų teikėju.

Archyvinė laiko žyma: ArchiveTimeStamp XAdES parašams, archive-time-stamp CAdES parašams, ar DocumentTimeStamp PAdES parašams.

Duomenų objektas: dvejetainiai / aštuntainiai duomenys, kuriuos programa apdoroja (pvz., transformuoja, skaičiuoja santrauką arba pasirašo) ir kurie gali būti susieti su papildoma informacija, pvz., identifikatoriumi, kodavimu, dydžiu ar tipu.

Egzistavimo įrodymas: įrodymas, kad objektas egzistavo specifiniu momentu (data/laikas).

Laiko žyma: elektroninės formos duomenys, kuriais kiti elektroninės formos duomenys susiejami su tam tikru laiku ir taip sukuriamas įrodymas, kad pastarieji egzistavo tuo metu (= elektroninė laiko žyma) [eIDAS].

Metaduomenys: duomenys apie kitus duomenis.

Pasirašantis asmuo: esybė, kuri yra skaitmeninio parašo sudarytoja.

Patikimas sąrašas: sąrašas, kuris pateikia informaciją apie patikimų paslaugų teikėjų patikimų paslaugų statusą ir statuso istoriją dėl atitikties taikomiems reikalavimams ir atitinkantis galiojančių teisės aktų nuostatas.

Sukompromitavimas: praradimas, vagystė, pakeitimas, neteisėtas naudojimas, ar kitoks konfidencialių duomenų saugumo pažeidimas.

Validavimo duomenys: duomenys, kurie yra naudojami skaitmeninių parašų validavimui.

ETSI – Europos Telekomunikacijų Standartų Institutas (*European Telecommunications Standardization Institute*)

OID – Objekto identifikatorius (*Object IDentifier*)

PS - Veiklos nuostatai (*Practice Statement*)

QLPS – Kvalifikuotos ilgalaikės apsaugos paslaugos (*Qualified Long-term Preservation Service*)

QTS - Kvalifikuotos patikimumo užtikrinimo paslaugos (*Qualified Trust Services*)

QTSP – Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjas (*Qualified Trust Service Provider*)

QTSS – Kvalifikuotos laiko žymų paslaugos (*Qualified Time-Stamping Service*)

RRT – Ryšių Reguliavimo Tarnyba

TSA – Laiko žymų tarnyba (*Time-Stamping Authority*)

4. MitSoft QTSP: Bendrosios sąvokos

MitSoft QTSP teikia tokias kvalifikuotas patikimumo užtikrinimo paslaugas:

- kvalifikuotas ilgalaikės apsaugos paslaugas;
- kvalifikuotą laiko žymų paslaugą.

MitSoft QTSP tenkina bendruosius reikalavimus patikimumo užtikrinimo paslaugų teikėjams, apibrėžtus standarte ETSI EN 319 401.

5. Rizikos vertinimas

MitSoft QTSP atlieka rizikos vertinimą tam, kad identifikuotų, analizuotų ir vertintų grėsmes veiklos turtui, atsižvelgdama į verslo ir techninius aspektus. Remiantis rizikos vertinimo rezultatais, pasirenkamos tinkamos rizikos mažinimo priemonės, kurios užtikrina, kad saugumo lygis atitiktų rizikos laipsnį.

QTSP nustato visus saugumo reikalavimus ir veiklos procedūras, kurios yra būtinos įgyvendinant pasirinktas rizikos mažinimo priemones, kaip dokumentuota „Informacijos saugumo taisyklėse" ir veiklos nuostatuose (QTS PS, QLPS PS, QTSS PS).

Rizikos vertinimą patvirtina ir liekamąją riziką priima MitSoft direktorius.

QTSP reguliariai (bent kartą metuose) peržiūri ir patikslina rizikos vertinimą.

6. TAISYKLĖS IR PRAKTIKOS

6.1. Kvalifikuotų patikimumo užtikrinimo paslaugų veiklos nuostatai

QTSP užtikrina ir demonstruoja būtiną patikimumą, teikiant kvalifikuotas patikimumo užtikrinimo paslaugas. Ypač:

a) Pagal paslaugų sutartį duomenų centras Rackray teikia MitSoft QTSP kvalifikuotų patikimumo užtikrinimo paslaugų sistemai infrastruktūros paslaugas. Rackray yra ISO 27001 sertifikuotas ir TIER3 Facility sertifikuotas duomenų centras.

   Duomenų centras „Interneto vizija" pagal sutartį teikia dedikuoto serverio paslaugas MitSoft QTSP duomenų nutolintų atsarginių kopijų kaupimui pagal sutartyje numatytas sąlygas.

b) Veiklos nuostatai ir kita dokumentacija, reikalinga įvertinti paslaugų atitiktį kvalifikuotų patikimumo užtikrinimo paslaugų taisyklėms, yra prieinama paslaugos abonentams ir pasikliaujančioms šalims MitSoft svetainėje ir pateikiama pagal paklausimą.

c) MitSoft direktorius yra atsakingas už QTSP veiklą su galutine teise patvirtinti Veiklos nuostatus.

d) MitSoft direktorius užtikrina praktikų įgyvendinimą, pavesdamas tai tinkamam personalui.

e) MitSoft QTSP turi Praktikų peržiūros procesą, apimantį Veiklos nuostatų priežiūrą.

f) QTSP tinkamai praneša apie ketinamus atlikti Veiklos nuostatų pakeitimus ir, juos patvirtinus pagal punktą c), pakeistus Veiklos nuostatus nedelsiant paskelbia, kaip tai reikalaujama pagal punktą b).

g) Paslaugų veiklos užbaigimo nuostatos yra pateiktos 7.12 skyrelyje „QTSP veiklos užbaigimas ir užbaigimo planai".

6.1.1. QTSP įsipareigojimai

6.1.1.1. QTSP įsipareigojimai abonentams

QTSP priima abonentų pretenzijas, kaip tai yra nurodyta skelbiamose Paslaugų teikimo sąlygose.

6.1.1.2. Atsakomybė

QTSP atsakomybė ir įsipareigojimai yra apibrėžti paslaugų teikimo Abonentinėje sutartyje.

6.1.1.3. Teisinės nuostatos ir interpretacijos

6.1.1.3.1. Pagrindiniai teisiniai aktai

Kvalifikuotų patikimumo paslaugų teikimas, reikalavimai teikėjams ir atsakomybė yra reguliuojami teisės aktais:

a) Europos Parlamento ir Tarybos Reglamente (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EC.

b) Lietuvos Respublikos Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų įstatymas, 2018 m. balandžio 26 d. Nr. XIII-1120.

c) Dėl Kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų ir kvalifikuotų patikimumo užtikrinimo paslaugų statuso suteikimo ir jų įrašymo į nacionalinį patikimą sąrašą bei kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų veiklos ataskaitų teikimo tvarkos aprašo patvirtinimo, Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. birželio 21 d. įsakymas Nr. 1V-588.

d) Dėl Pranešimų apie patikimumo užtikrinimo paslaugų saugumo ir (ar) vientisumo pažeidimus teikimo tvarkos aprašo patvirtinimo (Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. birželio 4 d. įsakymas Nr. 1V-594).

6.1.1.3.2. Ginčų sprendimas

Bet kokie ginčai tarp QTSP ir galutinių naudotojų yra sprendžiami geranoriškomis derybomis. Tuo atveju, jei ginčo išspręsti nepavyksta, yra kreipiamasi į teisėsaugos įstaigas.

6.1.1.4. Mokesčiai

QTSP gali nustatyti savo kvalifikuotų patikimumo užtikrinimo paslaugų kainas.

6.1.1.5. Intelektinės nuosavybės teisės

Cituojant bet kurį QTSP dokumentą, yra reikalaujama pateikti nuorodą į šaltinį.

6.2. Paslaugų teikimo sąlygos

QTSP skelbia visiems abonentams ir potencialioms pasikliaujančioms šalims kvalifikuotų patikimumo užtikrinimo paslaugų teikimo sąlygas.

Paslaugų teikimo sąlygos specifikuoja:

a) Teikiamų paslaugų naudojimo bet kuriuos apribojimus, įskaitant žalos atlyginimo apribojimus, kylančius iš paslaugų naudojimo viršijant šiuos apribojimus.
b) Abonentų įsipareigojimus.
c) Laikotarpį, kurį yra saugomi QTSP įvykių žurnalai.
d) Atsakomybės apribojimus.
e) Taikomą teisinę sistemą.
f) Skundų ir ginčų sprendimo procedūrą.
g) QTSP kontaktinius duomenis.
h) Bet kokius prieinamumo įsipareigojimus.

Ši informacija yra prieinama MitSoft interneto svetainėje lietuvių ir anglų kalbomis ir gali būti papildyta Abonentinėse sutartyse tarp QTSP ir abonentų.

6.3. Informacijos saugumo taisyklės

QTSP turi MitSoft direktoriaus patvirtintas informacijos saugumo taisykles, kurios nustato organizacijos informacijos saugumo valdymo metodą.

QTSP užtikrina, kad taikomos administracinės ir valdymo procedūros yra adekvačios ir atitinka pripažintą gerąją praktiką. Konfliktuojančios pareigos ir atsakomybės sritys yra atskirtos, siekiant sumažinti galimybes neleistinam ar netyčiniam QTSP turto modifikavimui ar piktnaudžiavimui.

QTSP yra atsakingas už visus kvalifikuotų patikimumo užtikrinimo paslaugų aspektus QTSP apimtyje, nepriklausomai nuo to, ar funkcijos yra perduotos

subrangovams ar ne. MitSoft QTSP yra atsakingas už visų šalių, dalyvaujančių kvalifikuotų patikimumo užtikrinimo paslaugų teikime, atitinkamų praktikų skelbimą.

Už informacijos saugumo gairių nustatymą, nuolatinę infrastruktūros priežiūrą, dokumentaciją, valdymą ir QTSP įrangos, patalpų, sistemų ir informacinio turto saugumo priemonių bei veiklos procedūrų įgyvendinimą, o taip pat informacijos ir kito turto apsaugą yra atsakingas MitSoft direktorius. QTSP užtikrina supažindinimą su saugumo gairėmis ir taisyklėmis visų susijusių darbuotojų, kuriems tai yra reikalinga jų darbe.

Įrangos, patalpų, sistemų ir informacinio turto, reikalingų kvalifikuotų patikimumo užtikrinimo paslaugų teikimui, saugumo priemonės ir veiklos procedūros yra dokumentuotos, valdomos ir įgyvendinamos.

Informacijos saugumo infrastruktūra, būtina saugumo užtikrinimui, yra nuolatos prižiūrima. Bet kurie įtakojantys saugumą pakeitimai yra tvirtinami MitSoft direktoriaus.

7. QTSP VALDYMAS IR VEIKIMAS

QTSP laikosi visų praktikų, nurodytų sekančiuose punktuose.

Kvalifikuotų patikimumo užtikrinimo paslaugų teikimas, atsakant į užklausas, yra vykdomas QTSP nuožiūra sutinkamai su paslaugų dokumentų ir Abonentinės sutarties nuostatomis.

7.1. Vidinė organizacija

7.1.1. Organizacijos patikimumas

QTSP užtikrina, kad ji yra patikima organizacija. Ypač:

a) QTSP pagal Lietuvos Respublikos teisę yra juridinis asmuo, įregistruotas juridinių asmenų registre kaip Uždaroji akcinė bendrovė "MIT-SOFT", įmonės kodas yra 120792080.

b) QTSP turi kokybės ir informacijos saugumo valdymo sistemą, tinkamą teikiamoms patikimumo užtikrinimo paslaugoms.

c) Ji įdarbinusi pakankamą skaičių darbuotojų, turinčių reikiamą išsilavinimą bei adekvačius mokymus, technines žinias ir patirtį kvalifikuotų patikimumo užtikrinimo paslaugų teikimui.

d) Taisyklės ir praktikos, pagal kurias QTSP veikia, yra paremtos tarptautiniais standartais ir nediskriminuojančios.

e) QTSP paslaugos yra prieinamos visiems naudotojams, kurių veikla patenka į deklaruotą veiklos sritį ir kurie sutinka priimti QTSP specifikuotus įsipareigojimus.

f) QTSP turi tinkamas priemones ir resursus, suderinamus su ES Reglamentu Nr. 910/2014 ir nacionaliniais įstatymais, padengti atsakomybei, kylančiai iš jo veiksmų ir veiklos.

g) QTSP turi finansinį stabilumą ir resursus, reikalingus veikti suderinamai su Veikos nuostatais, įskaitant reikalavimus QTSP veiklos užbaigimui.

h) Skundų ir ginčų sprendimo dėl kvalifikuotų patikimumo užtikrinimo paslaugų teikimo ar bet kokiais kitokiais susijusiais klausimais taisyklės ir procedūros yra specifikuotos kaip nustatyta Paslaugų teikimo sąlygose.

i) QTSP turi dokumentuotus susitarimus ir sutartinius santykius, su paslaugų teikime dalyvaujančiomis trečiosiomis šalimis.

7.1.2. Pareigų atskyrimas

Konfliktuojančios pareigos ir atsakomybės sritys yra atskirtos, kaip tai apibrėžta QTSP Informacijos saugumo taisyklėse (žr. 6.3 skyrelį „Informacijos saugumo taisyklės"), siekiant sumažinti galimybes neleistinam ar netyčiniam informacijos modifikavimui ar QTSP turto piktybiškam naudojimui.

7.2. Žmogiškieji ištekliai

QTSP užtikrina, kad personalas ir įdarbinimo praktikos išplečia ir remia QTSP veiklos patikimumą. Ypač:

a) QTSP įdarbina asmenis, kurie disponuoja ekspertinėmis žiniomis, patirtimi ir kvalifikacija, būtinomis siūlomoms paslaugoms ir tinkamomis veiklos funkcijoms atlikti.

b) Darbuotojams, pažeidžiantiems QTSP taisykles ir procedūras, yra taikomos drausminės nuobaudos.

c) Darbuotojų saugumo rolės ir atsakomybės, kaip tai yra nustatyta QTSP „Informacijos saugumo taisyklėse", yra dokumentuotos jų darbo aprašuose. Patikimos rolės, nuo kurių priklauso QTSP veikla, yra aiškiai identifikuotos.

d) QTSP darbuotojai (laikini ir pastovūs) turi darbo aprašus, apibrėžtus pagal pareigų atskyrimo ir būtinumo žinoti principus, nustatant darbo pozicijos jautrumą, remiantis pareigomis ir prieigos lygmenimis, išsilavinimu ir darbuotojo mokymais bei suvokimu. Darbo aprašai apima įgūdžių ir patirties reikalavimus.

e) Darbuotojai taiko administracines ir valdymo procedūras ir procesus, kurie dera su QTSP informacijos saugumo valdymo procedūromis.

f) QTSP įdarbina vadovaujančius darbuotojus, kurie disponuoja:
   - Skaitmeninių parašų kvalifikuotų ilgalaikės apsaugos technologijų žiniomis.
   - Skaitmeninių parašų technologijų žiniomis.
   - Darbuotojų su saugumo atsakomybėmis saugumo procedūrų žinojimu.
   - Informacijos saugumo ir rizikos vertinimo patirtimi.

g) Visi QTSP darbuotojai patikimose rolėse neturi interesų konflikto, kuris gali įtakoti QTSP veiklos nešališkumą.

h) Patikimos rolės yra apibrėžtos QTSP „Informacijos saugumo taisyklėse" ir apima roles, įtraukiančias šias atsakomybes:
   - Saugumo pareigūnas: saugumo praktikų įgyvendinimo administravimo bendra atsakomybė.
   - Sistemos administratorius: įgaliotas instaliuoti, konfigūruoti ir prižiūrėti kvalifikuotų patikimumo užtikrinimo paslaugų QTSP pasikliovimo sistemas.
   - Sistemos operatorius: atsakingas už QTSP pasikliovimo sistemų kasdienį veikimą. Įgaliotas atlikti sistemos atsarginių kopijų išsaugojimą ir atstatymą iš jų.
   - Sistemos auditorius: įgaliotas peržiūrėti QTSP pasikliovimo sistemų archyvus ir audito žurnalus.

i) QTSP darbuotojai yra už saugumą atsakingos vadovybės formaliai paskirti atlikti patikimas roles.

j) Darbuotojai neturi prieigos prie patikimų funkcijų tol, kol nebus atlikti būtini patikrinimai.

MitSoft direktorius yra atsakingas už įdarbinimą darbuotojų, tenkinančių visus šiuos reikalavimus, o taip pat už jų įgūdžių ir patikimumo patikrinimą, darbuotojų rolių apibrėžimą ir aprašymą (įskaitant patikimas funkcijas) jų darbo aprašuose.

Visi darbuotojai gali atlikti tik jų rolėse numatytas veiklas.

7.3. Turto valdymas

QTSP užtikrina, kad informacija ir kitas turtas yra tinkamai apsaugoti. Visų pirma, QTSP prižiūri viso turto sąrašą ir priskiria šiam turtui klasifikuotus apsaugos reikalavimus sutinkamai su rizikos analize.

Visi informacijos nešėjai yra tvarkomi saugiai pagal informacijos klasifikavimo schemos reikalavimus. Informacijos nešėjai, turintys jautrius duomenis, yra saugiai sunaikinami, kai tampa nebereikalingais.

7.4. Prieigos kontrolė

QTSP užtikrina, kad QTSP sistemų prieiga yra apribota tik tinkamai įgaliotiems asmenims. Konkrečiai:

a) Ugniasienė yra naudojama apsaugoti QTSP vidinio tinklo sritis nuo neleistinos prieigos, įskaitant abonentų ir trečiųjų šalių prieigą. Ugniasienė yra sukonfigūruota drausti visus nebūtinus QTSP veiklai protokolus ir prieigą. Techninis sprendimas yra pateiktas dokumente „Sistemos architektūra ir valdymas" (angl. „System architecture and management").

b) QTSP užtikrina efektyvų administravimą naudotojų prieigos, reikalingos operatorių, administratorių ir auditorių darbui. Tokiu būdu palaikomas sistemos saugumas, įskaitant MitSoft QTSP naudotojų paskyrų valdymą, auditą ir savalaikį prieigos modifikavimą arba pašalinimą .

c) Prieiga prie informacijos ir taikomosios sistemos funkcijų yra apribota sutinkamai su prieigos valdymo taisyklėmis, ir QTSP sistema užtikrina pakankamą saugumo kontrolę QTSP identifikuotų patikimų rolių atskyrimui, įskaitant saugumo administravimo ir eksploatavimo funkcijų atskyrimą. Ypač, yra apribotas ir pilnai kontroliuojamas sistemos tarnybinių programų (utilitų) naudojimas.

d) QTSP darbuotojai yra tinkamai identifikuojam ir autentifikuojami prieš naudojant kritines programas, susijusias su kvalifikuotomis patikimumo užtikrinimo paslaugomis.

e) QTSP darbuotojai yra atskaitingi už savo veiklą; šiuo tikslų, įvykių žurnalai yra išsaugomi (žr. 7.10 skyrelį „Įrodymų surinkimas").

f) Jautrūs duomenys yra apsaugoti nuo atskleidimo per pakartotinai naudojamus saugojimo objektus (pvz., pašalintus failus), kurie tampa prieinami neįgaliotiems naudotojams.

g) Lokalaus tinklo komponentės (pvz., maršrutizatoriai) yra saugomi saugioje fizinėje aplinkoje ir jų konfigūracija yra periodiškai audituojama QTSP specifikuotų reikalavimų atitikimui.

h) Naudojama nuolatinė stebėsena ir signalizacijos įrenginiai, siekiant įgalinti QTSP aptikti, registruoti ir laiku reaguoti į bet kokius neleistinus ir/ar neteisėtus prieigos prie resursų mėginimus.

7.5. Kriptografinis valdymas

Įdiegtos tinkamos saugumo kontrolės priemonės kriptografinių raktų ir kriptografinių įrenginių valdymui per visą jų gyvavimo ciklą.

7.6. Fizinis ir aplinkos saugumas

QTSP užtikrina, kad fizinė prieiga prie kritinių paslaugų yra kontroliuojama ir fizinė prieiga turtui yra minimizuota. Konkrečiai:

- Fizinė prieiga prie kvalifikuotų patikimumo užtikrinimo paslaugų yra apribota tik tinkamai autorizuotiems asmenims.
- Saugumo zonoje neautorizuotą asmenį lydi autorizuotas asmuo.
- Apsaugos priemonės yra įgyvendintos, siekiant išvengti turto praradimo, pažeidimo ar kompromitavimo, informacijos vagystės ar nutekinimo, verslo veiklų pertraukimo.
- Apsaugos priemonės yra įgyvendintos, siekiant išvengti informacijos ir informacijos apdorojimo įrangos kompromitavimo ar vagystės.

- Kvalifikuotų patikimumo užtikrinimo paslaugų įrenginiai veikia aplinkoje, kuri fiziškai apsaugo paslaugas nuo kompromitavimo per neleistiną prieigą prie sistemos ar duomenų.
- Fizinė apsauga yra pasiekiama sukūrus aiškiai apibrėžtą kvalifikuotų patikimumo užtikrinimo paslaugų saugumo perimetrą. Šio perimetro viduje nėra patalpų, kuriomis dalinamasi su kitomis organizacijomis.
- Fizinio ir aplinkos saugumo apsaugos priemonės yra įgyvendintos, siekiant apsaugoti sistemos resursų įrenginius, pačius sistemos resursus ir įrenginius, palaikančius jų veikimą. Kvalifikuotų patikimumo užtikrinimo paslaugų sistemos fizinio ir aplinkos saugumo taisyklės apima fizinę prieigos kontrolę, apsaugą nuo gamtinių nelaimių, priešgaisrinės saugos faktorius, palaikančių komunalinių paslaugų (elektros maitinimas, telekomunikacijos) trikius, struktūros griuvimą, vandentiekio nuotėkį, apsaugą nuo vagystės, įsilaužimą, atkūrimą nelaimės atveju.
- Apsaugos priemonės yra įgyvendintos, apsaugant įrangą, informaciją, nešėjus, programinę įrangą nuo išnešimo be leidimo.

QTSP kvalifikuotų patikimumo užtikrinimo paslaugų įranga veikia Rackray duomenų centre (DC). Tuo pačiu duomenų centro viduje yra apibrėžtas saugumo perimetras, į kurio vidų prieiga nėra galima. Duomenų centro pastatas yra saugomas apsauginių ir saugumo tarnybos. Kiekvienas patekimas į fiziškai saugią zoną ir išėjimas iš jos yra registruojamas. Tokiu būdu, QTSP turtas, įskaitant informacijos nešėjus, yra apsaugotas nuo neleistino paėmimo ar kompromitavimo.

Duomenų centre veikia moderni oro kondicionavimo sistema, kuri palaiko reikiamą oro temperatūrą ir valo orą nuo dulkių. Jeigu elektros tiekimas sutrinka, UPS ir dyzeliniai elektros srovės generatoriai palaiko normalų sistemos veikimą 4 val.

Tam, kad būtų išvengta kompromitavimo ir informacijos vagystės, yra imtasi šių priemonių: QTSP įranga, interneto ryšys yra apribotas – tik kvalifikuotų patikimumo užtikrinimo paslaugų teikimui būtinas ryšys yra leistinas. Ugniasienės ir įsilaužimo apsaugos sistemos yra įgyvendintos.

7.7. Veiklos saugumas

Kritinėms paslaugoms, kaip identifikuoja rizikos analizė, QTSP naudoja pasikliovimo sistemas ir produktus, kurie yra apsaugoti nuo modifikacijų. QTSP užtikrina, kad QTSP sistemos komponentės yra saugios ir korektiškai veikia su minimalia trikių rizika.

Konkrečiai:

a) Saugumo integravimo į IT sistemas tikslu saugumo reikalavimų analizė yra atlikta QTSP sistemos kūrimo projekto reikalavimų specifikavimo ir projektavimo etapų metu.

b) Pakeitimų valdymo procedūros yra taikomos visoms operacinės programinės įrangos laidoms, modifikacijoms ir atsirandantiems programinės įrangos pataisymams ir konfigūracijos pakeitimams, kuriems taikomos QTSP „Informacijos saugumo taisyklės", įskaitant konfigūracijos saugumo patikrinimus. Šios procedūros apima pakeitimų dokumentavimą. Maksimalus intervalas tarp dviejų konfigūracijos saugumo patikrinimų neviršija 12 mėnesių.

c) QTSP sistemos komponenčių ir informacijos integralumas yra apsaugotas nuo virusų, kenkėjiškos ir neleistinos programinės įrangos, įdiegtos antivirusinės programinės įrangos pagalba.

d) QTSP pasikliovimo sistemoje naudojami informacijos nešėjai yra saugiai tvarkomi, siekiant apsaugoti nešėjus nuo pažeidimų, vagystės, neteisėtos prieigos ir senėjimo.

e) Informacijos nešėjų valdymo procedūros yra naudojamos, siekiant apsaugoti informacijos nešėjus nuo pasenimo ir pablogėjimo per visą laikotarpį, kurį įrašus privaloma saugoti.

f) Procedūros yra parengtos ir įgyvendintos visoms patikimoms ir administracinėms rolėms, kurios įtakoja kvalifikuotų patikimumo užtikrinimo paslaugų teikimą.

g) Saugumo pataisymų valdymo procedūros yra naudojamos, siekiant užtikrinti:
   - saugumo pataisymų panaudojimą per pagrįstą laiko tarpą po to, kai jie tampa prieinami;
   - saugumo pataisymai nėra naudojami, jeigu jie iššaukia naujus pažeidžiamumus ar nestabilumą, kas nusveria jų panaudojimo naudą;
   - saugumo pataisymų nenaudojimo priežastys yra dokumentuotos.

h) Pajėgumų poreikiai yra stebimi ir numatomi būsimi pajėgumų reikalavimai, siekiant, kad adekvataus dydžio apdorojimo galia ir saugykla būtų prieinami.

7.8. Tinklo saugumas

QTSP prižiūri ir apsaugo QTSP pasikliovimo sistemą, patalpintą Rackray duomenų centre saugiame vidiniame tinkle ir prieinamą tik patikimų rolių darbuotojams. Tos pačios saugumo priemonės yra taikomos visoms sistemos komponentėms, išdėstytoms saugiame vidiniame tinkle:

a) QTSP segmentuoja patikimumo užtikrinimo paslaugų sistemos tinklą, remiantis QTSP „Informacijos saugumo taisyklių" reikalavimais, sutinkamai su funkcinėmis, loginėmis ir fizinėmis komponenčių priklausomybėmis, kaip pateikta dokumente „Sistemos architektūra ir valdymas".

b) QTSP apriboja prieigą ir komunikaciją tarp zonų, kurios yra būtinos QTSP veiklai.

c) QTSP sistemos konfigūracija yra sugriežtinta taip, kad tik būtinos paskyros, programos, paslaugos, protokolai ir portai yra naudojami.

d) QTSP „Informacijos saugumo taisyklės" identifikuoja patikimas roles ir priskiria atitinkamas atsakomybes tinkle saugumo praktikų įgyvendinimui. QTSP reguliariai peržiūri nustatytą saugumo taisyklių aibę.

e) QTSP talpina saugiose zonose visas QTSP veiklai kritines posistemes, kaip tai nurodyta dokumente „Sistemos architektūra ir valdymas".

f) QTSP atskiria IT sistemų administravimui dedikuotą tinklą nuo QTSP veiklos saugaus vidinio tinklo.

g) QTSP nenaudoja saugumo taisyklių administravimo sistemų kita paskirtimi.

h) QTSP atskiria QTSP paslaugų gamybinę sistemos aplinką nuo kūrimo ir testavimo sistemų aplinkų. Kūrimo ir testavimo sistemos yra patalpintos MitSoft patalpose ir įrenginiuose.

i) Pagal dokumentą „Sistemos architektūra ir valdymas" QTSP nustato komunikavimą tarp skirtingų posistemių tik patikimais kanalais, kurie yra logiškai skirtingi nuo kitų komunikavimo kanalų ir užtikrina kanalų galinių taškų saugų identifikavimą ir kanalo duomenų apsaugą nuo modifikavimo ir atskleidimo.

j) QTSP atlieka QTSP identifikuotų viešų ir privačių IP adresų pažeidžiamumo skenavimą.

k) QTSP atlieka įsiskverbimo į QTSP sistemą testavimą, įdiegus QTSP sistemą ir po infrastruktūros ar programų atnaujinimo ar modifikavimo, kurie QTSP vertinimu yra reikšmingi.

l) QTSP pateikia įrodymus, kad pažeidžiamumo skenavimą ir įsiskverbimo testavimą atliko asmenys, turintys įgūdžius, įrankius, patyrimą ir nepriklausomumą, būtinus patikimos ataskaitos pateikimui.

7.9. Incidentų valdymas

QTSP nuolat stebi prieigos prie QTSP paslaugų sistemos ir jos naudojimo veiklas:

a) Stebėsenos veiklos analizuoja sistemos būseną ir renka techninę informaciją, kuri yra riboto naudojimo pagal MitSoft QTSP informacijos klasifikavimo schemą ir yra prieinama tik asmenims patikimose rolėse su saugumo įsipareigojimais.

b) Nenormalus sistemos veikimas, kuris indikuoja potencialius saugumo pažeidimus, įskaitant galimą įsilaužimą, yra aptinkamas ir pranešamas kaip pavojaus signalas, remiantis stebėsenos funkcionalumu ir sistemos administratoriaus bei sistemos operatoriaus įsipareigojimais.

c) Stebėsena apima įvykių įrašų registravimo funkcijų darbo pradžią ir pabaigą bei reikiamų paslaugų QTSP tinkle prieinamumą ir naudojimą.

d) QTSP veikia savalaikiai ir koordinuotai tam, kad greitai reaguotų į incidentą ir apribotų saugumo pažeidimo poveikį, kaip tai aprašyta „Incidentų valdymo procedūroje".

e) QTSP pareigybių aprašuose priskiria sistemos administratoriaus patikimos rolės darbuotojams sekimą įspėjimų apie potencialiai kritinius saugumo įvykius ir užtikrinimą, kad apie atitinkamus incidentus būtų pranešama pagal QTSP procedūras.

f) QTSP nustato atitinkamų šalių informavimo procedūras pagal taikomas taisykles apie bet kokį saugumo pažeidimą ar integralumo praradimą, kuris turi reikšmingą poveikį patikimų paslaugų teikimui ir saugomiems asmens duomenims per 24 val. nuo pažeidimo identifikavimo.

g) QTSP pagal „Incidentų valdymo procedūrą" praneša fiziniams ar juridiniams asmenims apie saugumo pažeidimą ar integralumo praradimą be nepagrįsto delsimo, kai saugumo pažeidimas ar integralumo praradimas gali turėti neigiamos įtakos fiziniam ar juridiniam asmeniui, kuriam patikimumo užtikrinimo paslaugos buvo teikiamos.

h) QTSP sistema yra stebima, įskaitant stebėseną ar reguliarią audito žurnalų peržiūrą, siekiant identifikuoti kenkėjiškos veiklos požymius. QTSP įgyvendina automatinius audito žurnalų apdorojimo mechanizmus, kad įspėtų darbuotojus apie galimus kritinius saugumo įvykius. Sistemos auditorius veikia sutinkamai su „Sistemos audito procedūra".

i) QTSP eliminuoja bet kurį naują kritinį pažeidžiamumą per 48 valandas nuo jo atradimo.

j) Bet kuriam pažeidžiamumui QTSP nustato potencialaus poveikio kainą ir ja remiantis sudaro ir įgyvendina pažeidžiamumo švelninimo planą ar dokumentuoja faktinį pagrindą, kad pažeidžiamumas nereikalauja ištaisymo.

k) Incidentų pranešimo ir reagavimo procedūros yra taikomos tokiu būdu, kad saugumo incidentų žala ir veikimo sutrikimai būtų minimizuoti.

7.10. Įrodymų surinkimas

QTSP užtikrina, kad atitinkama informacija apie kvalifikuotų patikimumo užtikrinimo paslaugų veikimą yra užrašoma ir saugoma tinkamą laiko tarpą su tikslu pateikti įrodymus teisiniuose nagrinėjimuose. Konkrečiai:

a) Specifiniai įvykiai ir duomenys, kurie turi būti registruojami, yra dokumentuoti QTSP „Informacijos saugumo taisyklėse", įskaitant klientų kreipinius į operacijų API, paslaugų operacijas ir naudotojų interaktyvius veiksmus.

b) Einamųjų ir archyvinių įrašų apie kvalifikuotų patikimumo užtikrinimo paslaugų veiksmus konfidencialumas ir integralumas yra palaikomas.

c) Įrašai apie kvalifikuotų patikimumo užtikrinimo paslaugų veikimą yra pilnai ir konfidencialiai archyvuojami pagal QTSP skelbiamas praktikas.

d) Įrašai apie kvalifikuotų patikimumo užtikrinimo paslaugų veikimą yra prieinami, jei reikalaujama kvalifikuotų patikimumo užtikrinimo paslaugų korektiško veikimo įrodymo pateikimo teisiniam nagrinėjimui.

e) Tikslus laikas, kada buvo atliekamas laikrodžio patikslinimas, viršijantis 1 sekundę, yra registruojamas. Laikas, naudojamas fiksuoti įvykius audito žurnaluose, yra sinchronizuojamas su UTC bent kartą per dieną.

f) Įvykiai yra registruojami žurnaluose tokiu būdu, kad negalėtų būti lengvai panaikinti ar sugadinti (išskyrus, kai jie patikimai perduoti į ilgalaikio saugojimo informacijos laikmenas) reikalaujamą išlaikyti laiko tarpą.

g) Bet kuri apie abonentus išsaugota informacija yra laikoma konfidencialia, išskyrus atvejus, kai gaunamas abonento sutikimas jos platesniam skelbimui.

7.11. Veiklos tęstinumo valdymas

QTSP turi atnaujinamą veiklos tęstinumo planą, kuris imamas vykdyti nelaimės atveju. Įvykus nelaimei, veikimas atstatomas per tęstinumo plane numatytą terminą, pašalinant nelaimės priežastis, kurios gali pasikartoti (pvz., saugumo pažeidžiamumas), taikant tinkamas ištaisymų priemonėmis.

QTSP užtikrina, kad QTSP paslaugų saugumo pažeidimo atveju, atitinkama informacija pranešama abonentams ir pasikliaujančioms šalims.

7.12. QTSP veiklos užbaigimas ir užbaigimo planai

QTSP užtikrina, kad QTSP kvalifikuotų patikimumo užtikrinimo paslaugų teikimo užbaigimo atveju, bus siekiama sudaryti kuo mažiau trikdžių abonentams ir pasikliaujančioms šalims. QTSP turi atnaujinamą veiklos užbaigimo planą, pagal kurį, prieš baigiant kvalifikuotų patikimumo užtikrinimo paslaugų teikimą, yra įvykdomos mažiausiai šios procedūros:

a) QTSP pateikia informaciją apie paslaugų veiklos užbaigimą visiems abonentams, pasikliaujančioms šalims ir priežiūros įstaigai, panaudojant turimus kontaktinius duomenis, ne vėliau kaip prieš 3 mėnesius.

b) QTSP visiems subrangovams nutraukia leidimą veikti QTSP vardu, atliekant bet kurias funkcijas, susijusias su kvalifikuotų patikimumo užtikrinimo paslaugų teikimo procesu.

c) QTSP patikimai šaliai perduoda įsipareigojimą prižiūrėti įvykių žurnalą ir audito archyvus, būtinus QTSP korektiško veikimo demonstravimui pagrįstą laikotarpį.

d) Prieš QTSP užbaigiant paslaugų teikimą, QTSP siekia patikimų paslaugų teikimą esamiems klientams pagal galimybes perduoti kitam QTSP.

e) QTSP turi susitarimus padengti šių minimalių reikalavimų išpildymo kaštus tam atvejui, jei QTSP patiria bankrotą ar dėl kitokių priežasčių negali padengti kaštų pats.

f) Paslaugų užbaigimo atveju QTSP informuos įtakotas esybes ir, jeigu taikytina, perduos QTSP įsipareigojimus kitoms šalims.

7.13. Atitiktis

QTSP patvirtina, kad MitSoft kvalifikuotos patikimumo užtikrinimo paslaugos atitinka Taisykles ir Veiklos nuostatus. Tokiu būdu, QTSP prisiima visus Taisyklėse apibrėžtus įpareigojimus ir išpildo visus reikalavimus veikloms.

QTSP veiklos atitiktis Taisyklėms ir Veiklos nuostatams yra tikrinama pagal šiuos QTS PS ne rečiau kaip kas dvejus metus.

QTSP užtikrina atitiktį teisiniams reikalavimams. Konkrečiai:

a) Atitiktis ES Reglamentui Nr. 910/2014 [eIDAS] yra patvirtinama bent kartą per 24 mėnesius, vykdant akredituotos atitikties vertinimo organizacijos atliekamą auditą.

b) QTSP nenustato specialių naudojimosi paslaugomis reikalavimų, dėl kurių neįgalieji negalėtų naudotis paslaugomis. Vartotojo sąsają pateikia patikimumo užtikrinimo paslaugų kliento programinė įranga. Pati patikimumo užtikrinimo paslaugų sistema suteikia ribotą vartotojo sąsają administravimo tikslais.

c) QTSP užtikrina, kad būtų laikomasi Europos duomenų apsaugos direktyvos 95/46/EB reikalavimų, kaip ji įgyvendinama Lietuvos teisės aktais:
   - QTSP apdoroja duomenis kartu su komunikacijos atributais, kad būtų užtikrintos patikimumo užtikrinimo paslaugos ir įvykdyti taikomų standartų reikalavimai, įskaitant saugumo, apskaitos ir pajėgumų planavimo stebėseną.
   - Teikiant paslaugas, jokie kiti duomenys, įskaitant asmens duomenis, nėra renkami ir tvarkomi.
   - Imamasi atitinkamų techninių ir organizacinių priemonių, kad būtų išvengta neleistino ar neteisėto gautų duomenų tvarkymo, atskleidimo, atsitiktinio praradimo, sunaikinimo ar sugadinimo.
   - UAB "MitSoft" turi asmens duomenų tvarkymo taisykles, dalyvaujantys darbuotojai yra pasirašę konfidencialumo sutartis.

d) MitSoft QTSP paslaugų programinė įranga neturi vartotojo sąsajos, ji suteikia API, kuris turėtų būti naudojama iš kliento sistemos.

e) Veiklos nutraukimo planą turi patvirtinti Lietuvos Respublikos ryšių reguliavimo tarnyba (RRT), atliekanti Nacionalinės kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų priežiūros įstaigos funkcijas.